

Polynomials Having Sparse Multiples

A dissertation submitted in partial fulfillment
of the requirements of M.Tech.(Computer Science)
degree of Indian Statistical Institute, Kolkata

by

Suresh Kumar R

under the supervision of

Prof. Bimal Kumar Roy
Indian Statistical Institute
Kolkata-700 035.

23rd July 2001

Indian Statistical Institute

203, Barrackpore Trunk Road,

Kolkata-700 035.

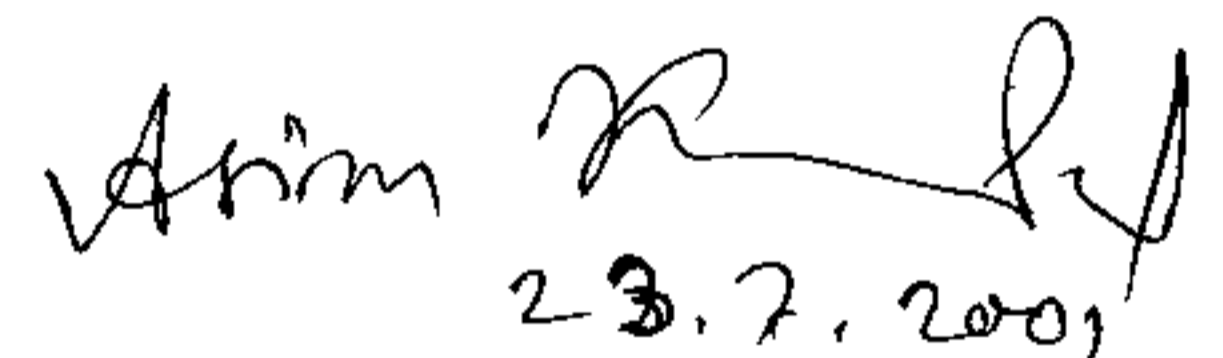
Certificate of Approval

This is to certify that this thesis titled "**Polynomials Having Sparse Multiples**" submitted by **Suresh Kumar R** towards partial fulfillment of requirements for the degree of M.Tech in Computer Science at Indian Statistical Institute, Kolkata embodies the work done under my supervision.



Bimal Kumar Roy,
Professor,
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata-700 035.

23.7.01



23.7.2001

(Prof. Asim Pal)

IIMC, Kolkata.

Acknowledgements

I take pleasure in thanking Prof Bimal Kumar Roy for his friendly guidance throughout the dissertation period. His pleasant and encouraging words have always kept my spirits up.

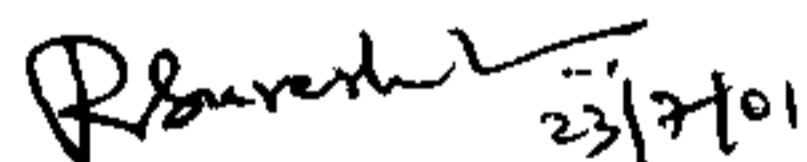
I would also like to express my sincere gratitude to Mr. Kishan Chand Gupta for agreeing to share a few words with me during few moments of intense pressure. A few days of conversation with him gave me a new confidence, enthusiasm and enabled me to sail successfully through the troubled waters of intense despair with renewed vitality.

I would also like to thank Mr. Jambunathan K for encouraging me to take this work.

I take pleasure in thanking Mr. Subhamoy Maitra for giving me his valuable time to share my views.

I would also like to thank Mr. Sandeepan Chowdhury for giving me the list of primitive polynomials and his prompt response.

Finally I take the opportunity to thank our classmates and our juniors for their kind nature in helping me to finish this work.


Suresh Kumar R

Contents

1	Introduction	1
1.1	Motivation	3
2	Preliminaries	4
2.1	Definitions	4
2.2	Notations	5
2.3	Relationship between $S_{l,d}$ and $C_{m,l}$	6
3	On Number of Cyclotomic Cosets	8
4	On Least Degree Trinomial Multiples	11
4.1	Algorithm for finding Least Degree Trinomial Multiple	11
4.2	List of Least Degree Trinomial Multiples of Primitive Polynomials	12

Chapter 1

Introduction

Stream ciphers form an important class of secret-key encryption schemes. They are widely used in applications since they present many advantages: they are usually faster than common block ciphers and they have less complex hardware circuitry. Moreover, their use is particularly well-suited when errors may occur during the transmission because they avoid error propagation. In a binary additive stream cipher the ciphertext is obtained by adding bitwise the plaintext to a pseudorandom sequence s , called the *key stream* (or the *running-key*). The running key is produced by a pseudorandom generator whose initialization is the secret key shared by the users. Most attacks on such ciphers therefore consist in recovering the initialization of the pseudorandom generator from the knowledge of a few cipher text bits (or of some bits of the running-key in known-plaintext attacks).

Linear feedback shift registers (LFSRs) are the basic components of most keystream generators since they are appropriate to hardware implementations, produce sequences with good statistical properties and can be easily analyzed.

Linear Feedback Shift Register (LFSR) is a system which generates a pseudorandom bit-sequence using a binary recurrence-relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{k-1} a_{n-k+1} + c_k a_{n-k} \quad (1.1)$$

where $c_k = 1$ and for $1 \leq i < k$, $c_i \in \{0, 1\}$. The length of a LFSR corresponds to the order k of the linear-recurrence-relation used. The number of taps t of an LFSR is the number of non-zero bits in $\{c_1, c_2, \dots, c_k\}$. The successive bits of the LFSR are emitted using the chosen recurrence relation after initializing the seed $(a_0, a_1, a_2, \dots, a_{k-1})$ of LFSR.

The (1.1) is related to the following polynomial over $\text{GF}(2)$

$$C(x) = 1 + c_1 x + c_2 x^2 + \dots + c_k x^k \quad (1.2)$$

The (1.2) is called the *Connection Polynomial* of the LFSR.

The LFSR-generated sequence of the linear-recurrence-relation (lrr) related to a connection polynomial is the same as the one for the corresponding lrr of multiple polynomial of the connection polynomial.

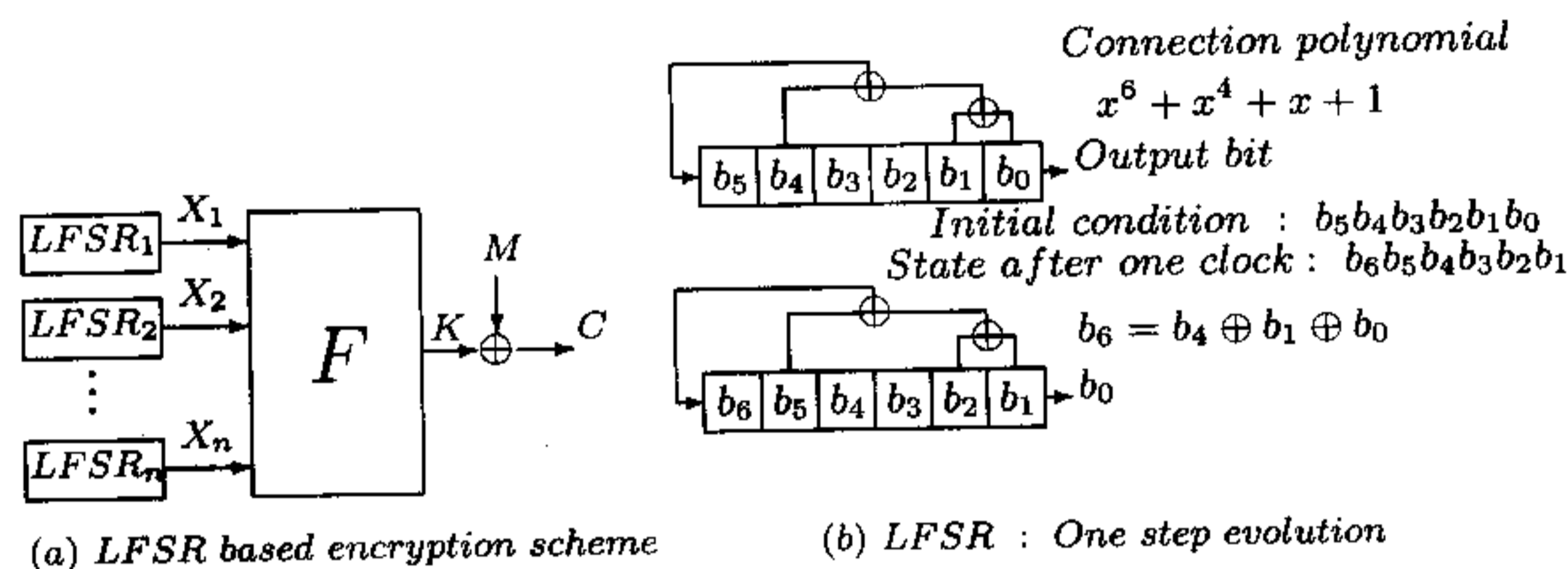


Figure 1.1: Stream Cipher System

In the stream-cipher systems, the key-stream is usually generated by combining the outputs of more than one LFSR using a nonlinear boolean function. This arrangement significantly increases the robustness of the system against possible attacks. This keystream is bitwise XORed with the message bitstream to produce the cipher. The decryption machinery is identical to the encryption machinery (see Figure 1.1).

In such a system, n bits from n different LFSRs are generated at each clock. These n bits are the input to the boolean function $F(X_1, X_2, X_3, \dots, X_n)$. The output of the boolean function F is the key-stream K . The cipher stream C is the XORing of K and the message stream M . i.e., $C = K \oplus M$.

Consider the connection polynomial of degree d

$$x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \dots + a_1x + 1 \quad (1.3)$$

where $a_i \in \{0, 1\}, \forall i, 1 \leq i \leq d - 1$. We take an LFSR corresponding to the connection polynomial of size d with least significant bit starts from the right hand side and the most significant bit at the leftmost position. There is a tap at i^{th} position if and only if $a_i = 1$. The output b , XORing of all taps is connected to the leftmost bit. The rightmost bit is the output of the LFSR system and all the bits are shifted by one bit towards the right hand side.

To resist cryptanalytic attacks on LFSR system, the connection polynomial must be primitive polynomial over $GF(2)$ with high weight and also there should not be any sparse multiple of moderate degree for the connection polynomial.

Various types of attacks exist on stream-cipher systems that use LFSRs for key-stream generation. These attacks try to infer the cryptosystem parameters i.e., the connection-polynomials and the seeds of the LFSRs using various known information like the statistical nature of the message source, the encrypted text, the actual combining-function used etc.

A category of these attacks, known as "fast-correlation" attack, assume that the number of LFSRs in the system and their connection-polynomials are

known. The attack takes the key-stream sequence i.e., the output of the combining function as input and tries to identify the seed of one of the LFSRs. The attack works only for those cases where the output-sequence of the attacked LFSR is strongly correlated¹ with key-stream. The attack views the key-stream sequence as a perturbation of the original LFSR sequence by a binary symmetric memoryless noise source with $\text{prob}(0)=\text{correlation probability}$. The "fast-correlation attack" algorithm (see [5]) for the attack systematically constructs atleast as many digits in the actual LFSR sequence as there are number of terms in the associated recurrence-relation. It uses these actual digits and the actual recurrence-relation employed and solves for the seed of LFSR using linear-algebra.

In [2], it has been shown that there exist exactly $2^{d-1} - 1$ distinct trinomial multiples of degree atmost $2^d - 2$ for a given primitive polynomial of degree d . We give an algorithm for finding the least degree trinomial multiple of a given primitive polynomial. We give the list of least degree trinomial multiples of their corresponding primitive polynomials. Also they proved that the number of cyclotomic cosets $\text{mod } (2^d - 1)$ of prime length p is $\frac{2^p - 2}{p}$. Here, we prove that the number of cyclotomic cosets $\text{mod } (2^d - 1)$ of length l , where l is any positive integer ($l > 1$) is

$$\frac{1}{l} \left[2^l + 2n - 4 - \sum_{i=1}^n 2^{\frac{l}{p_i}} + 2^{\text{gcd} \left(\frac{l}{p_1}, \frac{l}{p_2}, \dots, \frac{l}{p_n} \right)} \right],$$

where the prime factorization of l is $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $\alpha_i \geq 1, n \geq 1$.

1.1 Motivation

In the previous section, it was remarked that LFSR systems with their connection polynomials very sparse are particularly very vulnerable to various known attacks. There are trinomial multiples of very low degree for connection polynomial of high weight for a reasonable degrees.

The main motivation of this dissertation work is to find the primitive polynomials for designing "good" stream cipher system. My motivation in this effort is finding the least degree trinomial multiple of a given primitive polynomial.

¹two sequences are correlated if the probability that a randomly chosen bit in one sequence is same as the corresponding bit in the other sequence is > 0.5

Chapter 2

Preliminaries

2.1 Definitions

In this section, the definitions of basic terms and with some basic results which are used in this document are provided. Most of these definitions are taken from [6, 7, 8]. We denote the field of prime order p by $GF(p)$ and we denote the extension field of dimension d over $GF(p)$ by $GF(p^d)$. In the rest of document, the base field is $GF(2)$.

Definition : Galois Field of order p^d

Let p be a prime and let d be any positive integer. Then there exists a field (It is unique up to Isomorphism) of order p^d . This field is called *Galois Field of order p^d* and it is denoted by $GF(p^d)$.

The set $GF(2^d)^*$ of non zero elements of $GF(2^d)$ is a cyclic group under multiplication with a generator α and $\alpha^{2^d-1} = 1$. Generator α is called *Group Primitive Element* of $GF(2^d)$. $GF(2^d) = \{0, 1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{2^d-2}\}$.

Definition : Irreducible Polynomial over $GF(2)$

A polynomial of degree d is called an *Irreducible Polynomial over $GF(2)$* if it is not a product of two polynomials of degree $< d$ over the field $GF(2)$.

Definition : Primitive Polynomial over $GF(2)$

Let $f(x)$ be an irreducible polynomial of degree d . Then $f(x)$ is said to be a *Primitive Polynomial of degree d* if the roots of $f(x)$ are the generators of the field $GF(2^d)$.

The number of primitive polynomials is $\frac{\phi(2^d-1)}{d}$, where ϕ is an *Euler phi function*.

Definition : Euler phi function

The *Euler phi function* ϕ is defined by letting $\phi(n)$ be the number of positive integers less than or equal to n that are relatively prime to n , where n is any

positive integer.

The Euler phi function ϕ is completely determined by the properties : $\phi(mn) = \phi(m)\phi(n) \Leftrightarrow \gcd(m, n) = 1$ and $\phi(p^n) = p^{n-1}(p - 1)$, p prime, $n > 0$.

Definition : Polynomial belongs to an Exponent

Let $f(x)$ be a polynomial of degree d ($d \geq 1$) with $f(0) \neq 0$. Then there exists a least positive integer e ($e \leq 2^d - 1$) such that $f(x)$ divides $x^e - 1$. The e is called an exponent/order of the $f(x)$ and we say the polynomial $f(x)$ belongs to exponent e .

If $f(x)$ is a primitive polynomial of degree d then $f(x)$ belongs to an exponent $e = 2^d - 1$.

Definition : Cyclotomic Coset mod $(2^d - 1)$ of length l containing m

For a given positive integer d , *Cyclotomic Coset mod $(2^d - 1)$ of length l containing m* is defined as the set $\{2^x m \bmod (2^d - 1) | x = 0, 1, 2, \dots, (l - 1)\}$, where l and m are positive integers.

i.e., The cyclotomic coset containing m consists the elements $m, 2^1 m, 2^2 m, 2^3 m, \dots, 2^{(l-1)} m$ with $\bmod (2^d - 1)$ where l is the smallest positive integer such that $m 2^l \equiv m \bmod (2^d - 1)$.

Definition : t -nomial over $\text{GF}(2)$

A polynomial with t non zero terms, one of them being the constant term is called t -nomial, or in other words a polynomial of weight t .

Note that, in literature, by a polynomial with *sparse* weight generally means $t \leq 10$.

The general form of a *Trinomial* of degree m is $x^m + x^n + 1$, where m, n are positive integers and $m > n$.

Definition : Least Degree Trinomial Multiple of a Polynomial

Let $f(x)$ be a polynomial. Then the trinomial $x^m + x^n + 1$ of degree m is said to be the *Least Degree Trinomial Multiple of $f(x)$* if $f(x)$ divides $x^m + x^n + 1$ and if $t(x)$ is a trinomial multiple (of degree k) of $f(x)$ then $m \leq k$.

Definition : Maximal Divisor

A divisor m of l is said to be a *Maximal Divisor* if for every divisor k of l , $m < k < l$, m does not divide k .

2.2 Notations

In this section, the notations which are used in this document are provided.

1. Let l and d be any two positive integers.

Then the set $\{m | m(2^l - 1) \equiv 0 \bmod (2^d - 1), 1 \leq m \leq 2^d - 2\}$ is denoted by $S_{l,d}$.

i.e., $S_{l,d} = \{m | m(2^l - 1) \equiv 0 \bmod (2^d - 1), 1 \leq m \leq 2^d - 2\}$.

2. For a given positive integer d ,
The Cyclotomic Coset $\text{mod } (2^d - 1)$ of length l containing m is denoted by $C_{m,l}$.
i.e., $C_{m,l} = \{2^x m \text{ mod } (2^d - 1) \mid x = 0, 1, 2, \dots, (l - 1)\}$.
3. For a given set S , The cardinality of S is denoted by $|S|$.
ie., $|S|$ is number of elements in the set S .
4. If l divides m then we denote $l \mid m$.
5. We denote $\text{gcd}_{k|l, k \text{ is maximal}}(2^k - 1)$ for the greatest common divisor (GCD) of all numbers of the form $2^k - 1$, where k is maximal divisor of l . We define gcd of a number is 1. *i.e.*, if there is only one maximal divisor of l then $\text{gcd}_{k|l, k \text{ is maximal}}(2^k - 1) = 1$

2.3 Relationship between $S_{l,d}$ and $C_{m,l}$

In this section, I provide some results on the sets $S_{l,d}$ and $C_{m,l}$. We see the relationship between the sets $S_{l,d}$ and $C_{m,l}$.

Lemma 1 : Let l and d be any two positive integers such that $l \mid d$. Then $|S_{l,d}| = 2^l - 2$.

Proof : Since $l \mid d$, $(2^l - 1) \mid (2^d - 1)$. and hence $S_{l,d}$ can be written as the set $T = \{m \mid m \equiv 0 \text{ mod } \frac{(2^d - 1)}{(2^l - 1)}, 1 \leq m \leq 2^d - 2\}$.

Since the congruence $m \equiv 0 \text{ mod } \frac{(2^d - 1)}{(2^l - 1)}$ has $2^l - 2$ many number of non zero solutions in between 1 and $2^d - 2$. Therefore $|T| = 2^l - 2$. Hence $|S_{l,d}| = 2^l - 2$.

Corollary 1 : Let l, d_1 and d_2 be any three positive integers such that $l \mid d_1$ and $l \mid d_2$. Then $|S_{l,d_1}| = |S_{l,d_2}|$.

Proof : By lemma 1, $|S_{l,d_1}| = 2^l - 2$ and $|S_{l,d_2}| = 2^l - 2$ and hence $|S_{l,d_1}| = |S_{l,d_2}|$.

Lemma 2 : Let l_1, l_2 and d be any three positive integers such that $l_1 \mid l_2$, $l_1 \mid d$ and $l_2 \mid d$. Then $S_{l_1,d} \subseteq S_{l_2,d}$.

Proof : Let $x \in S_{l_1,d}$. Then x satisfies the congruence relation $x(2^{l_1} - 1) \equiv 0 \text{ mod } (2^d - 1)$ and hence $(2^d - 1) \mid x(2^{l_1} - 1)$. Since $l_1 \mid l_2$, $(2^{l_1} - 1) \mid (2^{l_2} - 1)$. By transitivity property, $(2^d - 1) \mid x(2^{l_2} - 1)$. This implies that x satisfies the congruence relation $x(2^{l_2} - 1) \equiv 0 \text{ mod } (2^d - 1)$ and hence $x \in S_{l_2,d}$.

Corollary 1 :

$$\bigcup_{k|l} S_{k,d} \subseteq S_{l,d}$$

Proof : The proof follows from the above Lemma 2.

Lemma 3 : Let d and l be two positive integers. Then for any integer m , $C_{m,l} \subseteq S_{l,d}$.

Proof : Let $x \in C_{m,l}$ then x satisfies the congruence $x(2^l - 1) \equiv 0 \pmod{2^d - 1}$. Therefore $C_{m,l} \subseteq \{x \mid x(2^l - 1) \equiv 0 \pmod{2^d - 1}, 1 \leq x \leq 2^d - 2\} = S_{l,d}$.

Corollary 1 :

$$\bigcup_m C_{m,l} \subseteq S_{l,d}$$

Proof : The proof follows from the above Lemma 3.

Lemma 4 : $C_{m,l} = C_{x,l}, \forall x \in C_{m,l}$.

Proof : Let $x \in C_{m,l}$. Since $x \in C_{x,l}$, so $C_{m,l} \subseteq C_{x,l}$. Let $y \in C_{x,l}$. Then $y = 2^k x \pmod{2^d - 1}$ for some integer k , $(0 \leq k \leq l - 1)$. Since $x \in C_{m,l}$, so $x = 2^q m \pmod{2^d - 1}$. Therefore $y = 2^{k+q} m \pmod{2^d - 1} \equiv 2^r m \pmod{2^d - 1}$, where r is the remainder when l divides $k + q$. Hence $C_{m,l} \subseteq C_{x,l}$.

Corollary 1 : $C_{m,l} \cap C_{x,l} = \emptyset, \forall x \notin C_{m,l}$.

Proof : Let $x \notin C_{m,l}$. Suppose $y \in C_{m,l} \cap C_{x,l}$. Then by above Lemma 4, $C_{m,l} = C_{y,l}$ and $C_{x,l} = C_{y,l}$. This implies that $C_{m,l} = C_{x,l}$ and hence $x \in C_{m,l}$. A contradiction. Hence the Corollary.

Chapter 3

On Number of Cyclotomic Cosets

In this chapter , I provide the result related to number of cyclotomic cosets for a given integer d .

Lemma 1:

$$\bigcup_m C_{m,l} = S_{l,d} - \bigcup_{k|l, k \text{ is maximal}} S_{k,d}.$$

Proof : Suppose $x \in \bigcup_m C_{m,l}$,

then $x \in C_{m,l}$ for some m . Let k be any maximal divisor of l . It is enough if we prove $x \notin S_{k,d}$. Suppose that $x \in S_{k,d}$ then x satisfies the congruence $x(2^k - 1) \equiv 0 \pmod{(2^d - 1)}$. Since $x \in C_{m,l}$, so l is the least positive integer such that $x(2^l - 1) \equiv 0 \pmod{(2^d - 1)}$, this implies that $l < k$, A contradiction.

$$\text{Hence } x \notin \bigcup_{k|l, k \text{ is maximal}} S_{k,d}.$$

We proved that

$$\bigcup_m C_{m,l} \subseteq S_{l,d} - \bigcup_{k|l, k \text{ is maximal}} S_{k,d}.$$

Now we will prove that

$$S_{l,d} - \bigcup_{k|l, k \text{ is maximal}} S_{k,d} \subseteq \bigcup_m C_{m,l}.$$

Let

$$x \in S_{l,d} - \bigcup_{k|l, k \text{ is maximal}} S_{k,d}.$$

Then x satisfies the $x(2^l - 1) \equiv 0 \pmod{2^d - 1}$ and $x \notin S_{k,d} \forall k$, k is a maximal divisor of l . Therefore $x \notin S_{q,d}$ for any proper divisor q of l (by Lemma2,Chapter 3). This implies that l is the least positive integer such that x satisfies $x(2^l - 1) \equiv 0 \pmod{2^d - 1}$ and hence $x \in C_{m,l}$.

Lemma 2:

$$\left| \bigcup_{k|l, k \text{ is maximal}} S_{k,d} \right| = \sum_{k|l, k \text{ is maximal}} |S_{k,d}| - (2^{\gcd_{k|l, k \text{ is maximal}} k} - 2)$$

Proof : Since the congruences $x(2^k - 1) \equiv 0 \pmod{2^d - 1}$, where k is maximal divisor of l are having $\gcd_k(2^k - 1) - 1$ many number of common non zero solutions of these relations, so we have

$$\left| \bigcup_{k|l, k \text{ is maximal}} S_{k,d} \right| = \sum_{k|l, k \text{ is maximal}} |S_{k,d}| - \gcd_{k|l, k \text{ is maximal}}(2^k - 1) - 1$$

Since $\gcd_k(2^k - 1) = 2^{\gcd_k k} - 1$ (see [8], volume 1, Chapter 4) So Lemma 2 holds.

Theorem 1 : The number of cyclotomic cosets $\pmod{2^d - 1}$ of length l , where l is any positive integer ($l > 1$) is

$$\frac{1}{l} \left[2^l + 2n - 4 - \sum_{i=1}^n 2^{\frac{l}{p_i}} + 2^{\gcd\left(\frac{l}{p_1}, \frac{l}{p_2}, \dots, \frac{l}{p_n}\right)} \right],$$

where the prime factorization of l is $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $\alpha_i \geq 1, n \geq 1$.

Proof : Let N be the number of cyclotomic cosets $\pmod{2^d - 1}$ of length l , where l is any positive integer ($l > 1$). By above Lemma 1,

$$\begin{aligned} \bigcup_m C_{m,l} &= S_{l,d} - \bigcup_{k|l, k \text{ is maximal}} S_{k,d} \\ \Rightarrow |\bigcup_m C_{m,l}| &= |S_{l,d}| - |\bigcup_{k|l, k \text{ is maximal}} S_{k,d}| \\ \Rightarrow |\bigcup_m C_{m,l}| &= |S_{l,d}| - \left[\sum_{k|l, k \text{ is maximal}} |S_{k,d}| - (2^{\gcd_{k|l, k \text{ is maximal}} k} - 2) \right] \\ \Rightarrow lN &= (2^l - 2) - \left[\sum_{k|l, k \text{ is maximal}} |S_{k,d}| - (2^{\gcd_{k|l, k \text{ is maximal}} k} - 2) \right] \end{aligned}$$

Let $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, ($\alpha_i \geq 1, n \geq 1$) be the prime factorization of l .

Then the maximal divisors of l are $\frac{l}{p_1}, \frac{l}{p_2}, \frac{l}{p_3}, \dots, \frac{l}{p_n}$.

$$\begin{aligned}
\text{So } lN &= (2^l - 2) - \left[\sum_i^n |S_{\frac{l}{p_i}, d}| - (2^{\gcd_i \frac{l}{p_i}} - 2) \right] \\
&= (2^l - 2) - \left[\sum_i^n (2^{\frac{l}{p_i}} - 2) - (2^{\gcd_i \frac{l}{p_i}} - 2) \right] \\
&= 2^l + 2n - 4 - \sum_i^n 2^{\frac{l}{p_i}} + 2^{\gcd_i \frac{l}{p_i}}
\end{aligned}$$

Hence

$$N = \frac{1}{l} \left[2^l + 2n - 4 - \sum_{i=1}^n 2^{\frac{l}{p_i}} + 2^{\gcd \left(\frac{l}{p_1}, \frac{l}{p_2}, \dots, \frac{l}{p_n} \right)} \right].$$

Corollary 1 : The number of cyclotomic cosets of prime length p is $\frac{2^p - 2}{p}$

Proof : Take $l = p$ in the above theorem. Then $n = 1$ and $N = \frac{1}{p}(2^p + 2 - 4 - 2 + 2) = \frac{1}{p}(2^p - 2)$.

Corollary 2 : For a given d , There are

$$\sum_{l|d, l=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}} \left[\frac{1}{l} \left(2^l + 2n - 4 - \sum_{i=1}^n 2^{\frac{l}{p_i}} + 2^{\gcd \left(\frac{l}{p_1}, \frac{l}{p_2}, \dots, \frac{l}{p_n} \right)} \right) \right]$$

many number of cyclotomic cosets.

Proof : By the proposition 3.1 of [2], cyclotomic cosets of length l exists $\Leftrightarrow l|d$. Hence the Corollary holds by above theorem.

Chapter 4

On Least Degree Trinomial Multiples

4.1 Algorithm for finding Least Degree Trinomial Multiple

In this section, an algorithm to find the Least Degree Trinomial Multiple (LDTM) for a given primitive polynomial is provided.

We represent primitive polynomial over $GF(2)$ as a string of 0's and 1's. Suppose (1.3) is a primitive polynomial of degree d . Then we can represent (1.3) as a string "1 a_{d-1} a_{d-2} a_{d-3} \cdots a_2 a_1 1" of length $d+1$. The input to this algorithm is a primitive polynomial with string representation. Let α be a root of the primitive polynomial.

Algorithm :

1. Generate alpha table up to degree d (*i.e.*, generate $\alpha^1, \alpha^2, \alpha^3, \dots, \alpha^d$)
2. $i = d + 1$
3. Find α^i and store the string α^i
(by using left shift operation on $\alpha^{(i-1)}$ and if the left most bit of $\alpha^{(i-1)}$ is '1' then bitwise XOR operation with α^d)
4. Compute $\alpha^i + 1$ (by XORing the rightmost bit of α^i with bit '1')
5. Search the alpha table for the string $\alpha^i + 1$.
If there is any string α^j equal to the string $\alpha^i + 1$, then $x^i + x^j + 1$ is the Least Degree Trinomial Multiple and terminate the program.
Otherwise increase the value of i by 1 and Go to Step 3

We suggest the following data structure to implement this algorithm.

```

struct GFElementNode
{
    int *Alpha; /* Alpha is a pointer to array which represents  $\alpha^i$  */
    long int Index; /* The power of  $\alpha$  (i.e.,  $\alpha^{Index}$ ) */
    struct GFElementNode *next; /* Pointer to next node  $\alpha^{(i+1)}$  */
};

```

In this algorithm, we are searching for the least degree trinomial constructing the alpha table on-the-fly. So we can allocate the space for GFElementNode whenever it is necessary. If we generate a 'reasonable' number of α^i 's before searching j then we can reduce the number of iterations required to search j . With the above proposed algorithm, we observed that the results are coming in a 'reasonable time' up to degree 32. The list of least degree trinomial multiples for some primitive polynomials of degree upto 32 is provided in section 4.2.

In [1], it has been shown that if $x^i + x^j + 1$ is a trinomial multiple of a primitive polynomial then i and j belong to the same length cyclotomic coset. Hence we can modify this algorithm slightly at step 5. Suppose i belongs to the cyclotomic coset of length l . We can search for j in cyclotomic cosets whose length is l .

4.2 List of Least Degree Trinomial Multiples of Primitive Polynomials

In this section, List of least degree trinomial multiples of corresponding primitive polynomials are provided. We represent polynomials in index form.

For example, If $x^{12} + x^6 + x^4 + x^1 + 1$ is a primitive polynomial of degree 12, then we write 12,6,4,1,0.

All primitive polynomials over GF(2) contains constant term $x^0 = 1$. So each polynomial (index form representation) contains 0. We denote LD TM for Least Degree Trinomial Multiple in the table.

Degree	Primitive Polynomial	LDTM
2	2,1,0	4,2,0
3	3,1,0	5,4,0
	3,2,0	5,1,0
4	4,1,0	8,2,0
	4,3,0	8,6,0
5	5,2,0	10,4,0
	5,3,0	10,6,0
	5,4,3,2,0	8,5,0
6	6,1,0	12,2,0
	6,4,3,1,0	8,7,0
	6,5,4,1,0	11,3,0
7	7,1,0	14,2,0
	7,4,3,2,0	10,9,0
	7,6,5,4,2,1,0	19,2,0
8	8,4,3,2,0	21,10,0
	8,7,6,5,4,2,0	13,2,0
	8,7,6,1,0	27,19,0
9	9,4,3,1,0	29,24,0
	9,7,5,4,2,1,0	27,15,0
	9,8,7,6,5,4,3,1,0	55,5,0
10	10,3,0	20,6,0
	10,9,8,4,2,1,0	55,14,0
	10,9,8,7,6,5,4,3,0	65,59,0
11	11,9,8,6,3,1,0	88,75,0
	11,10,9,8,7,6,5,4,0	101,19,0
	11,10,9,7,6,5,4,1,0	31,11,0
12	12,6,4,1,0	107,97,0
	12,10,9,8,6,1,0	115,2,0
	12,10,9,6,2,1,,0	161,84,0
13	13,4,3,1,0	94,13,0
	13,9,8,7,2,1,0	239,12,0
	13,12,11,10,9,8,7,6,5,1,0	141,82,0
14	14,5,3,1,0	224,77,0
	14,8,7,5,4,2,0	101,65,0
	14,11,10,9,8,7,5,4,3,1,0	266,265,0
15	15,1,0	30,2,0
	15,8,7,6,4,3,2,1,0	197,53,0
	15,12,10,9,4,2,0	644,561,0
16	16,5,3,2,0	567,543,0
	16,9,8,7,2,1,0	452,431,0
	16,14,12,11,8,7,6,5,4,3,2,1,0	461,368,0
17	17,3,0	34,6,0
	17,8,6,5,3,2,0	328,103
	17,14,12,8,6,5,3,1,0	682,493

Degree	Primitive Polynomial	LDTM
18	18,5,2,1,0	1347,1020,0
	18,10,5,4,3,2,0	313,94,0
	18,14,8,5,4,2,0	179,8,0
19	19,5,4,3,2,1,0	1549,540,0
	19,9,8,6,5,3,0	1241,669,0
	19,11,7,5,4,3,0	77,34
20	20,3,0	40,6,0
	20,9,8,7,6,5,4,3,2,1,0	1831,221,0
	20,10,8,7,4,3,2,1,0	667,588,0
21	21,2,0	42,4,0
	21,8,6,3,2,1,0	2531,2284,0
	21,9,8,4,3,1,0	3301,316,0
22	22,10,9,8,7,6,2,1,0	4871,598,0
	22,11,8,7,6,1,0	4102,343,0
	22,12,10,9,8,6,5,4,0	4279,122,0
23	23,5,0	46,10,0
	23,8,5,3,2,1,0	1434,171,0
	23,9,6,4,3,1,0	5375,0
24	24,4,3,1,0	5839,5530,0
	24,7,6,5,4,2,0	4422,3843,0
	24,23,20,16,15,10,9,6,5,3,2,1,0	4643,1498,0
25	25,3,0	50,6,0
	25,3,2,1,0	3590,1729,0
	25,24,22,18,17,16,12,9,6,5,4,2,0	15113,892,0
26	26,6,2,1,0	2603,476,0
	26,6,3,2,0	11141,6634,0
	26,25,24,23,22,21,17,15,14,11,8,7,5,2,0	21099,14702,0
27	27,8,5,4,0	1095,120,0
	27,8,6,4,3,2,0	28849,8192,0
	27,8,6,5,4,3,0	11441,9220,0
28	28,3,0	56,6,0
	28,6,4,1,0	34033,29967,0
	28,8,7,6,4,3,2,1,0	31160,12809,0
29	29,2,0	58,4,0
	29,20,11,2,0	31648,2719,0
	29,26,5,2,0	30587,27485,0
30	30,6,4,1,0	12033,1181,0
	30,8,4,1,0	18478,1017,0
	30,7,5,4,3,2,0	33558,24505,0
31	31,3,2,1,0	341,5,0
	31,6,0	62,12,0
	31,7,0	62,14,0
32	32,8,5,2,0	120301,73148,0
	32,9,5,3,0	56500,36121,0
	32,27,25,22,20,18,16,10,9,5,4,2,0	14632,6209

References and Tools

References

1. K.Jambunathan. On Choice of Connection Polynomials for LFSR based stream ciphers. In Progress in Cryptology - INDOCRYPT 2000, number 1977 in Lecture Notes in Computer Science, pages 9-18. Springer Verlag, 2000.
2. Kishan Chand Gupta and Subhamoy Maitra ,Primitive Polynomials over GF(2) - A Ctyptologic Approach.
3. Anne Canteaut and Michel Trabbia ,Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5.
4. Nirmal R.Saxena and Edward J. McCluskey, Degree- r Primitive Polynomial Generation- $O(r^3)$ $O(k r^4)$ Algorithms.
5. W.Meier and O.Staffelbach, Fast Correlation Attacks on Certain Stream-Ciphers, Journal of cryptology(1989) 1:159-176
6. Lidl R and Niederreiter Herald, Finite Fields, London Addison Wessley Publications 1983.(Encyclopaedia of Mathematics and it's applications v. 20).
7. Steven Roman, Field Theory,Graduate Texts in Mathematics,Springer Verlag,1995.
8. F.J.Mc.Willams and N.J.A.Sloane ,The Theory of Error Correcting Codes. North Holland, 1977

Tools

1. http://www-crc.stanford.edu/crc_papers/primitive.pdf
2. <http://www.theory.csc.uvic.ca/cos/gen/poly.html>
3. **Online-Calculations with the Crypto-Interpreter**
<http://ks.ferruni-hagen.de/~rieke/crypto/online.phtml.en>