FACTORIZATION OF POLYNOMIALS IN THE CONTEXT OF CODING THEORY

by

Loukas Komis

Submitted to the Department of Electrical Engineering

in partial fulfilment of the requirements for the degree

of

Master of Science

Department of Electrical Engineering

Faculty of Pure and Applied Science

University of Ottawa

OTTAWA , ONTARIO

JULY , 1971

ABSTRACT

The factorization of polynomials over GF (q) is an important consideration in the theory of error correcting codes .

The existing algorithms for the factorization of polynomials over Galois Fields are considered and a different approach is suggested for the case of q = 2 .

The suggested algorithm appears to be comparatively efficient when the degrees of the irreducible factors of the polynomials are not high .

A K N O W L E D G E M E N T S

I am very grateful to my advisor , Professor S. G. S. Shiva , for his guidance and assistance in the preparation of this work .

Thanks are also due to the members of the staff and the graduate students of the Department of Electrical Engineering for their encouragement throughout the past two years .

The financial assistance of the National Research Council of Canada and the University of Ottawa is gratefully aknowledged .

TABLE OF CONTENTS.

INTRODUCTION

In Engineering there are many cases in which one is required to factorize a polynomial. For example the necessity arises directly in the area of feedback Shift Register Sequences. Golomb [4] who has studied extensively this field states....." the factorization of polynomials over finite fields has found major technological applications, including secure, reliable and efficient communications, digital ranging and tracking systems, deterministic simulation of random processes and computer sequencing timing schemes. ".

In the area of Error Correcting Codes, Cyclic Codes form an important class. Among Cyclic Codes the Bose-Chaudhuri-Hocquenghen Codes are of extreme importance so far as random error correction is concerned. The properties and capabilities of all Cyclic Codes depend on the factors of their generator polynomial over some finite field. This class of Codes has been extensively studied by Peterson [15], Berlekamp [2], McWilliams [18] and many others. The recent advances in decoding techniques make these codes even more attractive from the practical point of view.

Furthermore, as stated by Berlekamp [1], some programming systems, such as Brown's ALPAK [20], deal with polynomials with integer coefficients. In these systems one is interested in the irreducible factors rather than the roots of them.

The problem also arises in another area of Error Correcting Codes, namely in the study of the Decomposition of Cyclic Codes into cyclic

classes, (see contributions by Goethals [19] and McWilliams [18]). In the recent contribution by Shiva et. al. [17] , one faces the problem of factoring the parity check polynomial h(x) into irreducible factors. The problem of Decomposition into cyclic classes is directly related to that of the weight distribution of a cyclic code. Further contributions on the same topic are due to Seguin [16].

In the design of Cyclic Codes the set of irreducible polynomials over some finite field must be known. These polynomials can be located as factors of a special class of binomials of the form $X^n - 1$, $n = q^i - 1$, $i = 1 , 2 , 3 , \ldots$ Therefore great effort has already been directed towards the factorization of these binomials. The results of the computations have been tabulated for relatively large i's [13], particularly for the case of $q = 2$, since in practice the polynomials over the binary field GF(2) are the ones that are mostly used.

In 1967 Berlekamp [1] presented an algorithm for factoring polynomials over any finite field; this algorithm treats the factorization of the previously mentioned binomials as a special case. The algorithm involves some matrix manipulations and the computation of a number of Greatest Common Divisors. We are going to discuss this algorithm in detail in Chapter II.

Shiva and Allard [7] have given some useful details on the technique introduced by Berlekamp for the case of the binomials of the mentioned form $X^q - 1$, $q = 2^i - 1$.

In 1969 McEliece [3] presented some results on the same topic; his algorithm is essentially similar to the one introduced by Berlekamp.

A few details about McEliece's algorithm will be given in Chapter II. In the same area some special cases have also been extensively studied. For example Golomb [4] has studied in detail the case of trinomials over finite fields in the context of his study on feedback Shift Register Sequences. Zierler [14] presented recently a method for locating the irreducible trinomials of the form $1 + X + X^n$ over GF(2) and tabulated the results of his computations for n up to 30,000.

Another extensively studied class of polynomials is the one of linearized and affine polynomials. They have been studied by Ore [5,6] who has even suggested a method for finding the roots of these polynomials.

In this thesis we are presenting a method for factoring a given polynomial over GF(2) into powers of irreducible polynomials. The suggested method reduces the problem to the computation of a series of Greatest Common Divisors.

As a first step the given polynomial is decomposed into square-free factors. A further step results in a decomposition into factors belonging also to some known binomial $X^n - 1$, $n = 2^i - 1$. The Cyclotomic polynomials over GF(2) are employed at the final step. The irreducible factors of the binomials of the form $X^q - 1$, $q = 2^i - 1$, are assumed to be known. In Chapter I we briefly give some necessary algebraic concepts essential for the material presented in the next Chapters. As we have already mentioned the existing methods are due to Berlekamp and McEliece. In Chapter II we present these algorithms in detail. In Chapter III we introduce another method for factoring polynomials over GF(2). Comments and concluding remarks are made in Chapter IV.

CHAPTER I

SOME ALGEBRAIC FUNDAMENTALS.

The most important known codes have a very strong algebraic structure. This is desirable because it facilitates the study of their properties and at the same time makes their implementation very interesting from the practical point of view. Consequently algebraic concepts form a very powerful tool in the study of Error Correcting Codes. In this Chapter we attempt to give the minimum algebraic prerequisites for the rest of this thesis.

This Chapter can be divided roughly in two parts; in the first parts we define the most significant algebraic structures along with some related important details; the second part deals with the fundamental concepts on polynomials over finite fields.

1. 1. GROUPS.

The first and most essential algebraic structure to be discussed is that of the Group.

The term ' binary operation ' on a set S , whenever used in the following discussion it will simply mean a mapping $f : S \times S \rightarrow S$, (includes the notion of algebraic closure on the set S.).

Definition 1. 1. 1. The Group.

A system $[G, o]$ consisting of a nonempty set G and a binary operation denoted by ' o ' and usually called ' multiplication ', is said to be a Group if the following postulates are satisfied :

(i) If $a, b, c \in G$ then, $(a o b) o c = a o (b o c)$.

(ii) There exists an element $e \in G$, called the left identity, such that, $e o a = a$, for every $a \in G$.

(iii) There exists an element $a^{-1} \in G$, for every $a \in G$, called the left inverse of a, such that, $a o a^{-1} = e$.

If a Group is also commutative, that is, if $a o b = b o a$, for every $a, b \in G$, then it is called an A b e l i a n G r o u p. If H is a subset of G and it is itself a Group, it is called a s u b g r o u p of G.

For example the set of all nonsingular matrices is a non-Abelian Group under the operation of matrix multiplication. The set of all real numbers is an Abelian Group under the ordinary operation of addition.

Definition 1. 1. 2. The Coset.

Let H be a subgroup of G and $a \in G$. The set,

$$a o H = \{ a o b \mid b \in H \}$$

is called a l e f t C o s e t of H. Respectively

$$H o a = \{ b o a \mid b \in H \}$$

is called a r i g h t C o s e t of H.

The number of elements of a Group G is called the o r d e r of G . The Group is called i n f i n i t e or f i n i t e as its order is infinite or finite respectively.

The power a^n of an element $a \in G$ is defined in the familiar way :

$$a^n = \underbrace{a \circ a \circ a \ldots\ldots \circ a}_{n}$$

A very important class of Groups is the one of Cyclic Groups .

Definition 1. 1 . 3. The Cyclic Group .

The o r d e r of an element $a \in G$ is the least positive integer m such that, $a^m = e$; if no positive power of a equals e , a has order infinity. The Group G is said to be C y c l i c if it contains some element x whose powers exhaust G ; this element is said to generate the Cyclic Group [10] .

1. 2. RINGS .

The second Algebraic structure to be discussed is that of the Ring. It is very important because it is directly related with the theory of polynomials.

Definition 1. 2. 1. The Ring .

A system [R, o, +] , consisting of a nonempty set R and two binary operations denoted by ' o ' and ' + ' and usually called ' multiplication ' and ' addition ' respectively, is said to be a Ring if the following postulates hold :

(i) The system $[R, +]$ is an Abelian Group.

(ii) $(a \circ b) \circ c = a \circ (b \circ c)$, for every $a,b,c \in R$.

(iii) $a \circ (b+c) = a \circ b + a \circ c$ and
$(b+c) \circ a = b \circ a + c \circ a$, for every $a,b,c \in R$.

A Ring is called c o m m u t a t i v e if it is so with respect to the operation 'o', that is, if $a \circ b = b \circ a$, for every $a,b \in R$. A R i n g w i t h i d e n t i t y is a Ring which possesses a multiplicative identity element. For example, the set of all positive and negative integers and zero form a commutative Ring with identity under the ordinary addition and multiplication. The set of all square matrices is a noncommutative Ring under matrix addition and multiplication.

Definition 1. 2. 2. The Ideal.

Let R be a Ring and I a subgroup of R under addition. I is called an Ideal if for every $a \in R$ and $b \in I$, then $a \circ b$ and $b \circ a \in I$. This is often called a two-sided Ideal. If I is such that, every element in I is a multiple of some $a \in I$, then I is said to be a p r i n c i p a l I d e a l .

The concept of the c h a r a c t e r i s t i c of an algebraic structure will be extensively used in our discussion on the finite fields; however it can already be introduced as the characteristic of a Ring with identity.

Definition 1. 2. 3. The characteristic of a Ring .

We call the characteristic of a Ring R the least positive integer m for which $\Sigma_{i=1}^{m} e = 1$, where e is the multiplicative identity element of the Ring R . [2] .

1. 3. FIELDS .

Definition 1. 3. 1. The Field .

A commutative Ring [F , o , +] with multiplicative identity element e is called a Field if for every nonzero element $a \in F$, there is a unique multiplicative inverse $a^{-1} \in F$.

It can be easily shown that the elements of a Field form an Abelian Group under addition as well as under multiplication. For example the sets of real numbers and complex numbers form Fields under the ordinary operations of addition and multiplication.

If both E and F are Fields and $E \supset F$, then F is said to be a subfield of E , and E an extension of F .

A very important class of Fields is the one of the so called Finite Fields . They are introduced after our discussion on Polynomials .

1. 4. VECTOR SPACES .

The concept of a vector space is essential for our discussion on the

existing algorithms for factoring polynomials over finite fields.

Definition 1. 4. 1. The Vector Space .

Let F be a Field. A Vector Space over F is a set V equiped with a binary operation called ' addition ' denoted by ' + ' and satisfying the following axioms.

(i) The system [V , +] is an Abelian Group .

(ii) For any $v \in V$ and $a \in F$, a ' product ' $a \circ v \in V$ is defined .

(iii) If $u, v \in V$ and $a \in F$, $a \circ (u + v) = a \circ u + a \circ v$.

(iv) If $v \in V$ and $a, b \in F$, $(a + b) \circ v = a \circ v + b \circ v$.

(v) If $v \in V$ and $a, b \in F$, $(a \circ b) \circ v = a \circ (b \circ v)$.

(vi) If $v \in V$, then $e \circ v = v$, where e is the multiplicative identity of F .

Let us consider an n-tuple $(a_1, a_2, a_3, \ldots, a_n)$ as an ordered set with elements in the Field F . We define a binary operation on it , called ' addition ' and denote it by ' + ', as follows :

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

The multiplication of an n-tuple by a field element c is defined as :

$$c \cdot (a_1, a_2, \ldots, a_n) = (c \circ a_1, c \circ a_2, \ldots, c \circ a_n).$$

With these two operations it can be easily verified that all n-tuples over a Field form a Vector Space over this Field and such a Vector Space plays a very important role in Coding Theory ; it is the only type of Vector Spaces that we are going to consider in the following discussion [15]. We should note that , the role of the additive identity element is played in such a Vector Space by the all-zero n-tuple .

A s u b s p a c e of a Vector Space V is a subset of V being itself a Vector Space .

A l i n e a r c o m b i n a t i o n of a finite number of elements of a Vector Space is an expression of the form : $\Sigma_{i=o}^{n} a_i v_i$, where $a_i \in F$ and $v_i \in V$. It is clear that such an expression , according to the Definition 1. 4. 1. , is also an element of V .

Definition 1. 4. 2. Linear Dependence .

A finite number of elements $v_1 , v_2 , \ldots , v_n$ of a vector space V over F is said to be l i n e a r l y d e p e n d e n t , if there exist elements $a_1 , a_2 , \ldots , a_n \in F$, not all zero , such that:

$$\Sigma_{i=1}^{n} a_i . v_i = 0 \quad ;$$

otherwise they are said to be l i n e a r l y i n d e p e n d e n t .

Definition 1. 4. 2. The Dimension of a Vector Space .

Dimension of a Vector Space V over F is the maximum number of linearly independent elements in it .

Suppose that the dimension of a Vector Space V is n and $v_1, v_2, \ldots, v_n \in V$, are linearly independent, then every element in V can be expressed as a linear combination of $v_1, v_2, \ldots, v_n$. The subset $v_1, v_2, \ldots, v_n$, is said to be a b a s i s for V and that it s p a n s or g e n e r a t e s the Vector Space V.

Every basis of the same Vector Space, can be shown, that it has the same number of elements ; this number is equal to the dimension of the Vector Space .

If E is an extension of the Field F, then it is a Vector Space over F. As such, it has a dimension over F, which may be infinite . This dimension is called the d e g r e e of E over F and it is denoted by [E : F], [24].

Furthermore, an i n n e r p r o d u c t or d o t p r o d u c t for two n-tuples over F , is defined as follows :

$$(a_1, a_2, \ldots, a_n) . (b_1, b_2, \ldots, b_n) = (a_1 . b_1 +$$

$$+ a_2 . b_2 + \ldots . + a_n . b_n)$$

Such an operation is commutative and distributive with respect to addition and the resulting sum belongs to F . If the inner product is equal to the additive identity element of F , the two n-tuples are said to be o r t h o g o n a l .

1. 5. POLYNOMIAL RINGS.

Let R be any commutative Ring with identity . An expression of

the form : $a_o + a_1 x + a_2 x^2 + \ldots + a_n x^n = \Sigma_{i=o}^{n} a_i x^i$, $a_i \in R$, is called a P o l y n o m i a l in x over R . The a_i' s are called c o e f f i c i e n t s of the polynomial and x its indeterminate .

For the Engineering applications , a polynomial over R may as well be regarded as a sequence (a_o , a_1 ,...., a_n) of elements of R . In the case of an all-zero sequence , we speak about a z e r o p o l y n o m i a l . [23]

We denote the set of all polynomials over R by R[x] . The greatest index n for which , the corresponding coefficient a_n is different than zero , is called the d e g r e e of the polynomial . The coefficient a_n is said to be the l e a d i n g c o e f f i c i e n t of the polynomial .

In the sequence representation of a polynomial , its degree is not necessarily equal to the length of the sequence ; the coefficients corresponding to indices greater than the degree of the polynomial may simply be equal to zero . If a polynomial of degree n has the leading coefficient a_n equal to 1 ,is called m o n i c .

Let us consider two elements $f(x) = \Sigma_{i=o}^{n} a_i x^i$ and $g(x) = \Sigma_{i=o}^{m} b_i x^i$ in R [x] ; we define two binary operations called ' polynomial addition ' and ' polynomial multiplication ' , denoted by ' + ' and ' o ' respectively in the following way :

$$(i) \quad f(x) + g(x) = \Sigma_{k=o}^{n} (a_k + b_k) x^k, \quad n > m ,$$

$$(ii) \quad f(x) o\, g(x) = \Sigma_i \Sigma_j a_i b_j x^{i+j} ,$$

It can be easily shown that the set $R[x]$ equipped with the previously defined operations satisfy the postulates of the Definition 1. 2. 1. and therefore the system $[R[x], +, o]$ is a commutative Ring, usually called the Polynomial Ring over R . The elements of the Ring R form a subring of $R[x]$ under the binary operations defined on R and we agree to call the elements of R constant Polynomials or simply constants .

Definition 1. 5. 1. The roots .

Let f(x) be a polynomial of degree n over a Field F . An element $a \in E$, where E is an extension of F, is called a root of f(x) if $f(a) = 0$.

The concept of the roots of a polynomial over a Field is directly related with the following Definition and Theorem .

Definition 1. 5. 2. The Splitting Field .

An extension E of a field F is a Splitting Field for a polynomial $f(x) \in F[x]$, if f(x) can be expressed as a product of linear factors in E , that is , $f(x) = c.(x - a_1).(x - a_2)\ldots.(x - a_n)$, $a_i \in E$ and E is the smallest extension of F containing the set of the roots $(a_1, a_2, \ldots a_n)$ [24]. It is evident that all a_i's are roots of f(x) , and that any extension of E is also a splitting field for f (x) .

Theorem 1. 5. 1.

A polynomial of degree n over F has at most n roots in some extension field of F. [2].

If a factor $(x - a_i)$ appears m times in the decomposition of $f(x)$ in linear factors in a splitting field E , is said that $a_i \in E$ is an m-times r e p e a t e d r o o t , or a root with multiplicity m . The concept of irreducibility in the polynomial ring is analogous to that of a prime integer in the ring of ordinary integers ; it is defined as follows :

Definition 1. 5. 3. The Irreducibility .

A polynomial $f(x) \in F[x]$ is said to be reducible over F , if $f(x) = a(x) \cdot b(x)$ for some nonconstant $a(x), b(x) \in F[x]$. Otherwise $f(x)$ is said to be i r r e d u c i b l e over F .[22]

We should note that the reducibility or irreducibility of a given polynomial depends heavily on the field F under consideration . Thus $1 + x^2$ is irreducible over the real field , whereas over the complex field or a field of characteristic 2 , $1 + x^2$ is reducible . The decomposition of reducible polynomials over a field F , into irreducible factors is guaranteed by the following Unique Factorization Theorem .

Theorem 1. 5. 2.

Every non-constant polynomial $f(x) = \Sigma_{i=o}^{n} a_i x^i$ can be factored as a product $f(x) = a_n f_1(x) \cdot f_2(x) \ldots f_k(x)$
where $f_i(x)$ are monic irreducible polynomials in $F[x]$.
The factors $f_i(x)$ are unique apart from the order they appear in the product [9].

If some $f_i(x)$ appears m times in the product , we say that it is

an m-times r e p e a t e d f a c t o r or a factor of multiplicity m . A polynomial with no repeated factors is sometimes called a s q u a r e-f r e e polynomial . In the next Chapters we are going to make extensive use of the concept of the Greatest Common Divisor of two polynomials over a field F . It is defined as follows :

Definition 1. 5. 4. The Divisibility

Let $f(x)$, $p(x) \in F[x]$. $f(x)$ is said to divide $p(x)$ if there exists a polynomial $h(x) \in F[x]$ such that $p(x) = f(x) \cdot g(x)$. We write $f(x) \mid p(x)$. If $f(x)$ does not divide $p(x)$ we write $f(x) \nmid p(x)$. [23]

Definition 1. 5. 5. The Greatest Common Divisor .

Let $g(x)$, $f(x)$, $p(x) \in F[x]$. If $g(x)$ is the monic polynomial of greatest degree such that $g(x) \mid f(x)$ and $g(x) \mid p(x)$, $g(x)$ is said to be the Greatest Common Divisor of $f(x)$ and $p(x)$ over F. [15]

The definition of the Greatest Common Divisor in the polynomial ring over F is analogous to the one defined for the ring of integers . It is similarly computed by the Euclidean Algorithm .

1. 6. FINITE FIELDS .

A field with a finite number of elements is called a F i n i t e F i e l d . Similarly, if an extension of a field is a finite field, is said to be a Finite extension of it .

The following theorems establish the existence and basic properties of finite fields .

Theorem 1. 6. 1.

The c h a r a c t e r i s t i c of a Field must be either infinity or p r i m e number p.[2]

Theorem 1. 6. 2.

The o r d e r of a Finite Field is a power of its characteristic .[2]

Theorem 1. 6. 3.

If p is a prime and n a positive integer , then there exists a Finite Field of p^n elements.[2]

Definition 1. 6. 1. The Galois Field .

A field of p^n elements (p and n as in Th . 1. 6. 3.) is called a G a l o i s F i e l d and is denoted by G F (p^n) .

Theorem 1. 6. 4.

G F (p^n) is a subfield of G F (p^m) iff n | m.[2]

Any Galois field of p^n elements may be considered as a finite extension of a finite field of p elements and therefore regarded as a vector space over the field of p elements which is sometimes called the g r o u n d F i e l d of G F (p^n) .
There is a finite group associated with every Galois Field , called the Galois Group of this Field , with the following important property .

Theorem 1. 6. 5.

The multiplicative Group of the nonzero elements of GF (p^n) is c y c l i c . [10]

Theorem 1. 6. 6.

The polynomial $x^q - x$, where $q = p^n$, has as roots all the elements of GF (q) . [22]

Therefore this special class of binomials has a set of roots forming a cyclic Group and all these nonzero roots can be expressed as powers of a generating element of this Group . This element must have order q-1 and is said to be a p r i m i t i v e element . Furthermore a polynomial over GF (p), which has a primitive element of GF (q) as a root is itself called a p r i m i t i v e p o l y n o m i a l .

Generally in any Field F , the elements satisfying the equation $x^n = 1$, are called the n th r o o t s o f u n i t y . If it so happens that $m = p^n$, where p is a prime , then the roots of unity according to Theorem 1. 6. 6. are the nonzero elements of GF (p^n) . Since the elements of GF (p^n) are distinct the binomials of the type $x - x^q$, where $q = p^n$, have no repeated roots and of course , no repeated factors .

The following important Theorem holds for the roots of any irreducible polynomial over a Finite Field.

Theorem 1. 6. 7.

Let $f(x)$ be an irreducible polynomial of degree n over $GF(q)$ and β a root of $f(x)$. Then $\beta, \beta^q, \ldots\ldots, \beta^{q^{n-1}}$, are all roots of $f(x)$. [15]

Theorem 1. 6. 8.

Every polynomial of degree m irreducible over $GF(q)$ is a factor of $x^{q^m} - x$. [15]

Some more Theorems on Galois Fields will be discussed in Chapter III, in parallel with the results which are directly related with them.

CHAPTER II

THE EXISTING ALGORITHMS.

In this Chapter we shall attempt a review on the two existing methods for factoring polynomials over Galois Fields . It has already been mentioned that these two algorithms are due to Berlekamp [1] , and McEliece [3]. They have both made the observation that a special class of polynomials , namely the one satisfying the relation :

$$[\,h(x)\,]^q - h(x) \equiv 0 \bmod f(x) \ ,$$

has a very interesting property regarding the factorization of a given f(x) over GF (q) . Both algorithms , therefore , have a common basic Theorem , but take somehow different approaches for generating polynomials h(x) satisfying the above relation. At the final step both algorithms make use of the Euclidean Algorithm for the computation of a number of Greatest Common Divisors resulting in the complete factorization of f(x) .

2. 1. THE BASIC THEOREM.

The following Theorem is the fundamental idea in both Berlekamp' s and McEliece' s algorithms .

Theorem 2. 1. 1.

Let f(x) and h(x) be two polynomials over GF (q). If ,

$$[\,h(x)\,]^q - h(x) \equiv 0 \bmod f(x) \ , \quad \text{then} \ , \quad f(x) = \prod_{s \in GF(q)} [\,g.c.d.(\,f(x)\ ,\ h(x) - s\,)\,] \qquad (\,2.\,1.\,1.\,)$$

Proof .

Since $[h(x)]^q - h(x) \equiv 0 \bmod f(x)$, $f(x)$ divides $[h(x)]^q - h(x)$.

But according to Theorem 1. 6. 6. $[h(x)]^q - h(x) = \prod_{s \in GF(q)} [h(x) - s]$.

Therefore $f(x)$ also divides $\prod_{s \in GF(q)} \{g.c.d.[f(x), h(x) - s]\}$. On the other hand g. c. d. $[f(x), h(x) - s]$ divides $f(x)$. If $s \neq t$ and $s, t \in GF(q)$, then $h(x) - s$ and $h(x) - t$ are relatively prime, as are g. c. d. $[f(x), h(x) - s]$ and g. c. d. $[f(x), h(x) - t]$. Therefore

$\prod_{s \in GF(q)} \{g.c.d.[f(x), h(x) - s]\}$ divides $f(x)$. We may assume that both polynomials are monic, therefore since each divides the other, they must be equal . [1 , 2]

Remark 2. 1. 1.

The only case that the factorization in Theorem 2. 1. 1. is trivial is that of $h(x)$ being a scalar . If $h(x)$ has positive degree , the factorization is nontrivial . However , in general this factorization is incomplete , because g. c. d. $[f(x), h(x) - s]$ may be reducible .

Definition 2. 1. 1. The f-reducing polynomials .

If Theorem 2. 1. 1. does give a nontrivial factorization of $f(x)$, we say , that such an $h(x)$ is an f-reducing polynomial .

There are two possible ways that an algorithm based on Theorem 2. 1. 1. could work . We could find just one f-reducing polynomial and then inductively proceed to find reducing polynomials for the

resulting factors ; or we could produce such a number of f-reducing polynomials , that they themselves would be enough to reduce all factors of f (x) . Both Berlekamp and McEliece prefer the second alternative which apparently shortens the procedure . In the next section , the two different approaches for obtaining f-reducing polynomials are described .

2. 2. BERLEKAMP ' S APPROACH .

Given a polynomial f (x) over GF (q) of degree m , the following three steps should be followed :

Step 1.

We form a square mxm matrix Q over GF(q) , in such a way , that the i th row of the matrix Q is the vector representation of the polynomial $x^{q(i-1)} \bmod f(x)$. In other words the following relation must hold :

$$x^{qi} \equiv \Sigma_{k=o}^{m-1} Q_{i+1,k+1}\, x^k \bmod f(x) \qquad (2.\ 2.\ 1.)$$

The previously defined matrix Q can be used for computing the residue $[h(x)]^q \bmod f(x)$, where $f(x) = \Sigma_{i=0}^{m-1} h_i x^i$, in any polynomial over GF(q) of degree less than m . This is accomplished by multiplying the row vector $(h_o , h_1 , \ldots , h_{m-1})$, corresponding to h(x) , by the matrix Q . This observation follows from the next relations :

Since q is the characteristic of GF(q), we have ,

$$[h(x)]^q = h(x^q) = \Sigma_{i=o}^{m-1} h_i x^{qi} \qquad (2.\ 2.\ 2.)$$

But according to the relation (2. 2. 1.)

$$\Sigma_{i=o}^{m-1} h_i x^{qi} \equiv \Sigma_{i=o}^{m-1} [\Sigma_{i=o}^{m-1} h_i Q_{i+1,\, k+1} x^k] \bmod f(x) , \quad (2. 2. 3.)$$

or $$\Sigma_{i=o}^{m-1} [\Sigma_{k=o}^{m-1} h_i Q_{i+1,k+1} x^k] = \Sigma_{i=o}^{m-1} [\Sigma_{i=o}^{m-1} h_i Q_{i+1,k+1}] x^k ,$$

finally $$[h(x)]^q \equiv \Sigma_{i=o}^{m-1} [\Sigma_{i=o}^{m-1} h_i Q_{i+1,k+1}] x^k \bmod f(x) , \quad (2. 2. 4.)$$

Similarly we could compute $[h(x)]^q - h(x) \bmod f(x)$ by multiplying the row vector $(h_o , h_1 , \ldots , h_{m-1})$ by the matrix $Q - I_m$, where I_m is the m-dimensional identity matrix over GF(q) .

Step 2.

At this point we should introduce the concept of the null-space of a vector subspace .

Definition 2. 2. 1. The null-space .

The set of all vectors o r t h o g o n a l to a subspace V_1 of a vector space V , forms another subspace of V , called the null-space of V_1 . [15]

Step 2 is as follows : We find a set of vectors which spans the null-space of $Q-I_m$. This may be done by appropriate elementary row and column operations on the matrix $Q-I_m$. Each polynomial in the determined basis of the null-space of $Q-I_m$ has a polynomial representation h(x) which satisfies the relation :

$$[h(x)]^q - h(x) \equiv 0 \bmod f(x) , \quad (2. 2. 5.)$$

and conversely every $h(x)$ satisfying the relation (2. 2. 5.) is represented by a row vector in the null-space of $Q - I_m$.

Step 3 .

Since we have a set of polynomials satisfying the assumption of Theorem 2. 1. 1. we may proceed to the factorization by applying the Euclidean Algorithm for the computation of the Greatest Common Divisors between $f(x)$ and $h(x)-s$ for each $s \in GF(q)$. When we apply Euclid 's Algorithm to $f(x)$ and $h^{(1)}(x)-s$, where $h^{(1)}(x)$ is some vector of the basis of the null-space of $Q-I_m$, the obtained factorization is not in general complete . We would be able to know if the factorization was complete , if we knew the number of irreducible factors of $f(x)$. This will be possible after the following Theorem , due also to Berlekamp [1].

Theorem 2. 2. 1.

The number of distinct irreducible factors of $f(x)$ is equal to the dimension of the null-space of $Q-I_m$.

But the dimension of the null-space of $Q-I_m$ is equal to the number of the vectors in some basis of that subspace : since we already have found such a basis , we automatically know the number of distinct irreducible factors of $f(x)$. Suppose that the dimension of the null-space of $Q-I_m$ is n ; if the first g. c. d. results in fewer than n factors of $f(x)$, then we compute the g. c. d. between some $h^{(2)}(x)-s$ and each known factor of $f(x)$. By this process we eventually locate all n irreducible factors of $f(x)$.

2. 3. McELIECE 'S APPROACH.

As we have already mentioned this approach is a slightly different way of constructing f-reducing polynomials for the final application of Theorem 2. 1. 1 It is a less general method of attacking the problem ; however a sufficient number of f-reducing polynomials is quaranteed for the complete separation of the irreducible factors of f(x) . At this point we should define the concept of the "exponent" of a polynomial since it is extensively used by McEliece .

Definition 2. 3. 1. The Exponent of a Polynomial .

The smallest positive integer e such that f(x) $|x^e-1$ is called the exponent of f(x) .

The set of f-reducing polynomials is introduced by the following definition .

Definition 2. 4. 2.

For each i, $1 \leq i < e$, let m_i the least integer such that ,

$$x^{iq^{m_i}} - x^i \equiv o \mod f(x) , \quad (2. 3. 1.)$$

we define the set of polynomials ,

$$R_i (x) \equiv x^i + x^{iq} + \ldots + x^{iq^{m_i-1}} \mod f(x) , \quad (2. 3. 2.)$$

Clearly every R(x) satisfies the relation $[R_i(x)]^q - R_i(x) \equiv o \mod f(x)$ of Theorem 2. 1. 1. because of the relation [2. 3. 1] and therefore the $R_i(x)$ ' s are candidates for f-reducing polynomials . The next step is to prove , that the number of f-reducing polynomials provided by the above definition 2. 3. 2 is sufficient for the complete factorization of f(x) over GF (q) .

The special case of $f(x) = x^e - 1$ is considered first and we shall see that this is enough for the generalization for any $f(x)$. The case of $x^e - 1$ is dealt by the following Theorem presented by McEliece [3].

Theorem 2. 3. 1.

Let $f_1(x)$ and $f_2(x)$ be two distinct irreducible divisors of $x^e - 1$. Then there is an integer i, $1 \leq i < e$, and distinct elements $a, b \in GF(q)$ such that

$$R_i(x) - a \equiv o \mod f_1(x), \qquad [2. 3. 3.]$$
$$R_i(x) - b \equiv o \mod f_2(x)$$

Hence the factors $f_1(x)$ and $f_2(x)$ can be "separated" by the factorization given in Theorem 2. 1. 1. Note that since $a \neq b$ $R_i(x) - a$ and $R_i(x) - b$ are relatively prime. The proof of Theorem 2. 3. 1. is based on two Lemmas given again by McEliece [3] and will not be presented here. However, we shall present the generalization of this Theorem in the form of a direct Corollary.

Corollary 2. 3. 1.

For any square-free polynomial $f(x)$, the corresponding $R_i(x)$, $1 < i < e$, will separate all the irreducible factors of $f(x)$.

Proof

Denote by $R_i^{(e)}(x)$, the $R_i(x)$'s associated with $x^e - 1$. Theorem 2. 3. 1. shows that the $R_i^{(e)}(x)$'s suffice to separate all factors of

$x^e - 1$, so they certainly suffice to separate the factors of $f(x)$

because , $x^{iq^m} - x^i \equiv 0 \bmod x^e - 1$, implies that , $x^{iq^m} - x^i \equiv 0 \bmod f(x)$, since $f(x)$ divides $x^e - 1$.

Q.E.D.

Therefore we are arriving at the conclusion that the set of the f-reducing polynomials as defined in Definition 2. 3. 2. suffices for the complete factorization of $f(x)$.

CHAPTER III

3. 1. ANOTHER APPROACH .

In this Chapter we propose a different approach to the problem of factorization of polynomials over Galois Fields . The class of binomials is excluded . The irreducible factors of $1 + x^n$, $n = 2^i - 1$, $i = 1, 2, ..$ can be reasonably assumed to be known since they are tabulated in the relevant literature [15 , 13]

The procedure is essentially a sequence of computations of suitably chosen Greatest Common Divisors between polynomials over GF(2). Some useful details , techniques and criteria will be given . The concept of the formal derivatives of polynomials is essential for the future discussion and will be studied below .

3. 2. FORMAL DERIVATIVES OF POLYNOMIALS .

Let $f(x) = a_o + a_1 x + a_2 x^2 + ... + a_n x^n$, be a polynomial over a field F . The first derivative $f'(x)$ of $f(x)$ is defined as follows :

Definition 3. 2. 1. The formal derivatives .

The polynomial $f'(x) = a_1 + 2.a_2.x + ... + n.a_n x^{n-1}$, where ' . ' denotes the operation of multiplication as defined for the field F , is said to be the first formal derivative of the polynomial f(x) .

If the polynomial is over the field of real numbers , this derivative agrees with the usual derivatives as defined in Calculus . From the Definition 3. 2. 1. , without any use of limits , one can deduce that many of the laws of the ordinary differentiation , such as ,

$$[f(x) + g(x)]' = f'(x) + g'(x)$$

$$[f(x) . g(x)]' = f'(x).g(x) + f(x).g'(x) ,$$

and so on , are obeyed .

The following important Theorem describes the behaviour of the multiple roots and factors of a polynomial over GF(2) , with respect to its first formal derivative .

Theorem 3. 2. 1.

Let f(x) be a polynomial over GF(2) and f'(x) its first formal derivative , assumed to be different than zero . An irreducible factor of f(x) of multiplicity n , is also a factor of f'(x) of multiplicity :

(i) n , if n is even .

(ii) n - 1 , if n is odd .

The proof of the above Theorem is given in Appendix A . Somewhat more generalized versions of this Theorem can be found in references [2] and [10] . The following Corollary will be used extensively in the rest of this discussion .

Corollary 1 .

Let $d(x)$ = g. c. d. $\{f(x)$, $f'(x)\}$, then the polynomial $A(x) = \frac{f(x)}{d(x)}$ has no repeated factors .

Proof .

A root of $f(x)$ of multiplicity e , will have multiplicity e or e-1 in $f'(x)$, acording to Theorem 3. 2. 1. , and therefore e or e-1 in $d(x)$. Hence it cannot appear more than once in $\frac{f(x)}{d(x)}$.

Q. E. D.

Atthis point we note that $f'(x)$ is zero only if $f(x)$ has all of its terms even powered . But in that case $f(x)$ can be written in the form

$f(x) = [p(x)]^{2^i}$, $i = 1, 2, \ldots$. Since the terms of $p(x)$ cannot be all even powered , it has a nonzero first formal derivative ,

therefore it can replace $f(x)$. The above transformation can be performed by simple inspection of $f(x)$. For example , if $f(x) = 1 + x^4 + x^8$, it can be written in the form , $f(x) = (1 + x + x^2)^{2^2}$, after an inspection of the powers of its terms .

3. 3. Separation of the multiple factors .

The first step of the suggested algorithm leads to an incomplete factorization of the given $A_o = \Sigma_{i=o}^{n} a_i x^i$ over $GF(2)$, into powers of factors containing no repeated roots . In case $A_o(x)$ has a zero first formal derivative , as we have mentioned before , we write $A_o(x)$ in the form $[A(x)]^{2^i}$ and proceed in the application of the algorithm with $A(x)$ instead of $A_o(x)$.

We apply the Euclidean Algorithm and compute the following sequence of Greatest Common Divisors .

$$\text{g. c. d. } \{ A_o(x) , A_o'(x) \} = [A_1(x)]^{2^{j_1}} , \qquad (3.3.1.)$$

$$\text{g. c. d. } \{A_1(x) , A_1'(x) \} = [A_2(x)]^{2^{j_2}} ,$$

. . . . . .

$$\text{g. c. d. } \{A_k(x) , A_k'(x) \} = [A_{k+1}(x)]^{2^{j_{k+1}}} = 1$$

The transformations on the right sides of the relations (3. 3. 1.) into the form $[A_i(x)]^{2^{j_i}}$ is also performed by inspection . The computations end when we meet some $A_k(x)$, relatively prime with its first formal derivative , which indicates the absence of more multiple factors . After the computations in the relations (3. 3. 1.) we note that $A_o(x)$ can be expressed in the following form :

(3. 3. 2.)

$$A_o(x) = \frac{A_o(x)}{[A_1(x)]^{p_1}} \left[\frac{A_1(x)}{[A_2(x)]^{p_2}}\right]^{p_1} \left[\frac{A_2(x)}{[A_3(x)]^{p_3}}\right]^{p_1 p_2} \cdots \left[\frac{A_{k-1}(x)}{[A_k(x)]^{p_k}}\right]^{p_1 \cdots p_{k-1}},$$

We define , $p_i = 2^{j_i}$, i = 0, 1, 2, ... , and $B_i(x) = \dfrac{A_i(x)}{[A_{i+1}(x)]^{p_{i+1}}}$ (3. 3. 3.)

Then the relation (3. 3. 2.) can be written in the form :

$$A_o(x) = B_o(x) [B_1(x)]^{p_1} \cdots [B_{k-1}(x)]^{p_1 p_2 \cdots p_{k-1}}, \quad (3.3.4.)$$

Each $B_i(x)$ contains no repeated factors . This can be easily seen from the definition of the $B_i(x)$ in the relations (3. 3. 3.) . Each $[A_{i+1}(x)]^{p_{i+1}}$ is the g. c. d. between $A_i(x)$ and its formal derivative . Therefore according to Theorem 3. 2. 1. and Corollary 1. $B_i(x)$ must be square-free . However , the factorization in the relation (3. 3. 4.) is incomplete because each $B_i(x)$ is in general still reducible over GF(2) .

3. 4. THE SEPARATION OF THE FACTORS OF EQUAL DEGREE .

We can further refine the factorization of the relation (3. 3. 4.) by partitioning the irreducible factors of each $B_i(x)$ into groups of factors of the same degree . This can be done by performing the following computations of g. c. d. ' s , for each $B_i(x)$, i = 0, 1, 2, ..k-1 .

$$\text{g. c. d.} \left[B_i(x) \, , \; 1 + x^{n_1} \right] = C_{i1}(x) \qquad , \; n_1 = 2^1 - 1 \, ,$$

$$\text{g. c. d.} \left[\frac{B_i(x)}{C_{i1}(x)} \, , \; 1 + x^{n_2} \right] = C_{i2}(x) \qquad , \; n_2 = 2^2 - 1 \, ,$$

. . . . . .

$$\text{g. c. d} \left[\frac{B_i(x)}{\prod_{j=1} C_{ij}(x)} \, , \; 1 + x^{n_m} \right] = C_{im}(x) \qquad , \; n_m = 2^m - 1 \, ,$$

(3. 4. 1.)

According to Theorem 1. 6. 8. , all the irreducible polynomials of degree m are factors of the binomial $1 + x^{2^m - 1}$. Therefore each $C_{ij}(x)$ contains all the irreducible factors of degree j of the polynomial $B_i(x)$. It does not contain factors of lower degree , because they have already been removed and included in some preceding $C_{ik}(x)$, j>k . It does not also contain factors of higher

than j degree , since none of them is a factor of $1 + x^{2^j - 1}$ or any preceding binomial with lower j . Therefore taking into account the powers in the relation (3. 3. 4.) and the partition performed in (3. 4. 1.) we can write the original polynomial in the form :

$$A_o(x) = [\, D_s(x) \,]^{d_s} [\, D_{s-1}(x) \,]^{d_{s-1}} \ldots . [\, D_1(x) \,]^{d_1} , \quad (3. 4. 2.)$$

Where each $D_j(x)$ divides some known binomial $1 + x^{2^j - 1}$, and is relatively prime to every other binomial of lower j . In other words every $D_i(x)$ contains irreducible factors of the same degree only .

At this point we can also find the number of irreducible factors of $A_o(x)$. If $D_i(x)$ divides $1 + x^{2^j - 1}$ and suppose that the number of irreducible factors of $[\, D_i(x) \,]^{d_i}$ is n_i , then we have ,

$n_i = d_i \dfrac{\text{deg. } D_i(x)}{j}$, and the number of irreducible factors of $A_o(x)$ will be $n = \Sigma_{i=1}^{s} n_i$.

However the factorization in (3. 4. 2.) may still be incomplete . If two or more factors of $A_o(x)$ of the same degree occur in the same $B_i(x)$ in (3. 3. 4.) , then they cannot be separated by the suggested factorization in (3. 4. 2.) .

We can further refine the factorization if we make use of the properties of the Cyclotomic Polynomials . The basic properties of these will be presented in the following section .

3. 5. CYCLOTOMIC POLYNOMIALS .

The Cyclotomic Polynomials are defined recursively as follows :

Definition 3. 5. 1.

The Cyclotomic Polynomial $\psi_i(x)$ is defined as : $\psi_i(x) = \dfrac{1 + x^i}{\prod_{j|i} \psi_j(x)}$.

It can be easily seen that the above definition results in an incomplete factorization of the binomial $1 + x^i$. For example for the case of $1 + x^{63}$, since 1, 3, 7, 9, 21, and 63 are the divisors of 63 , we have :

$$\psi_1(x) = 1 + x \ ,$$

$$\psi_3(x) = \frac{1 + x^3}{\psi_1(x)} \ ,$$

$$\psi_7(x) = \frac{1 + x^7}{\psi_1(x)} \ ,$$

$$\psi_9(x) = \frac{1 + x^9}{\psi_1(x)\ \psi_3(x)} \ ,$$

$$\psi_{21}(x) = \frac{1 + x^{21}}{\psi_1(x)\ \psi_3(x)\ \psi_7(x)} \ ,$$

$$\psi_{63}(x) = \frac{1 + x^{63}}{\psi_1(x)\ \psi_3(x)\ \psi_7(x)\ \psi_9(x)\ \psi_{21}(x)} \ ,$$

and therefore : $1 + x^{63} = \psi_1(x)\ \psi_3(x)\ \psi_7(x)\ \psi_9(x)\ \psi_{21}(x)\ \psi_{63}(x)$.

This is a partition of the factors of $1 + x^{63}$ and of the elements of $GF(2^6)$

according to certain rules , which we are going to discuss in this section .

The following Theorem is sometimes used as an alternative definition of the Cyclotomic Polynomials .

Theorem 3. 5. 1.

The field elements which are roots of a Cyclotomic Polynomial have the same order . [2]

A consequence of the above Theorem is that , all the irreducible factors of a Cyclotomic Polynomial have the same degree . The degree of a Cyclotomic Polynomial and the degree of its irreducible factors can be determined without finding or factoring the Cyclotomic Polynomial itself , by applying the following Theorems .

Theorem 3. 5. 2.

If $n = \prod_i p_i^{e_i}$, where all p_i's are primes , then deg $\psi_n(x) = \phi(n)$, where $\phi(n)$ is the Euler's phi function , given by $\prod_i p_i^{e_i - 1}(p_i - 1)$. [2]

Theorem 3. 5. 3.

The degree of the irreducible factors of $\psi_n(x)$ over GF(2) , is equal

to the multiplicative order of 2 mod n .

For example, in the case of $\psi_{63}(x)$ we have , $63 = 3^2 . 7$, then $\phi(63) = 3 . (3-1) . 7^0 . (7-1) = 36$. Therefore deg $\psi_{63}(x) = \phi(63) = 36$. We also have that , $2^6 \bmod 63 = 1$, which means that the multiplicative order of 2 mod 63 is 6 . Therefore we can conclude that $\psi_{63}(x)$ has 6 irreducible factors of degree 6 .

3. 6. SEPARATION OF FACTORS OF EQUAL EXPONENT .

As we have mentioned the factorization of the relation (3. 4. 2.) may , in general , result in some reducible factors of $A_o(x)$, but each $D_i(x)$ will contain factors of the same known degree . However , it may happen , that these irreducible factors belong to different exponents . In this case , these factors can be separated by computing the g. c. d. ' s between the $D_i(x)$ and the relevant Cyclotomic Polynomials . More specifically , if $D_d(x)$ contains factors of degree d , we locate these Cyclotomic Polynomials which contain irreducible factors of degree d , according to Theorem (3. 5. 3.) . Let these Cyclotomic Polynomials be $\psi_{n_1}(x)$, $\psi_{n_2}(x)$, . . . , $\psi_{n_1}(x)$. Then we compute the following g. c. d. 's :

$$\text{g. c. d. } \{ D_d(x) , \psi_{n_j}(x) \} = E_{dj}(x) \quad , \quad j = 1, 2, \ldots, 1 .$$

Each $E_{dj}(x)$ will contain irreducible factors of degree d and belonging to the exponent j .

The factorization will not be complete in the case that some $D_i(x)$ contains irreducible factors of the same degree , and at the same time , belonging to the same exponent .

For example , if $D_i(x) = (1 + x + x^2 + x^3 + x^4) (1 + x + x^4)$, a complete factorization is possible because the exponent of $1 + x + x^2 + x^3 + x^4$ is 5 , therefore $(1 + x + x^2 + x^3 + x^4) \mid \psi_5(x)$; but the exponent of $1 + x + x^4$ is 15 and therefore , $(1 + x + x^4) \mid 1 + x^{15}$ and no binomial of the form $1 + x^n$ for $n < 15$. However , the complete factorization would not be possible if $D_i(x) = (1 + x + x^4) (1 + x^3 + x^4)$ because both factors of $D_i(x)$ belong to the exponent 15 .

Therefore if at this step if we face the case of some $D_i(x)$ containing irreducible factors of the same exponent , we have to choose between the two alternatives as described in the following :

(i) Make use of the tables of irreducible polynomials over GF (2) . Since we know the degree and the number of irreducible factors of each $D_i(x)$, by trial and error we determine which irreducible polynomials of the given degree divide the respective $D_i(x)$.

(i i) Since $D_i(x)$ divides some know binomial of the form $1 + x^{2^m - 1}$, where m is the degree of the irreducible factors of $D_i(x)$ over GF (2), then all the roots of $D_i(x)$ must be distinct elements of GF (2^m). We generate, therefore, the Galois field GF (2^m) and try each of its elements to determine if it is a root of $D_i(x)$. It is enough to locate only one root of $D_i(x)$ in order to separate an irreducible factor of $D_i(x)$, because if for example β is such an element of GF (2^m), then $\beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}$ will also be roots of the same irreducible factor of $D_i(x)$. Therefore each irreducible factor of $D_i(x)$ will be of the form :

$$f_i(x) = (x + \beta)(x + \beta^2) \ldots (x + \beta^{2^{m-1}}).$$

The sets of roots of irreducible polynomials over GF (2) dividing $1 + x^{2^m - 1}$ are disjoint, consequently there will be no possibility of confusion in determining the roots of each irreducible factor of $D_i(x)$.

We should note that the generation of GF (2^m) is an easy procedure and the required circuit is very simple. In case that the procedure is computerized, this alternative also appears quite attractive. The related software approach is given in Appendix B.

3. 7. AN EXISTENCE CRITERION FOR NONTRIVIAL G. C. D. 'S .

In case we wish to make sure that two polynomials have a g. c. d. different than 1 before applying the Euclidean Algorithm , we may use the following classical criterion , which will help us to avoid the computation of unecessary g. c. d. 's .

Let P (x) and Q (x) be the two polynomials of degrees p and q respectively . Let H be the square (p + q) x (p + q) matrix constructed the following way : The first q rows are P (x) , x P (x) ,..., x^{q-1} P (x) and the remaining P rows are Q (x) , x Q (x) ,..., x^{p-1} Q (x) . Then the following Theorem holds.

Theorem 3. 7. 1.

The value of the determinant of H is zero iff [P (x) , Q (x)] ≠ 1 . [25]

The proof of the above Theorem is given in Appendix A .
The computation of such a determinant over GF (2) is rather easy requiring a certain number of row operations on H which , in the GF (2) case , are nothing but modulo 2 vector additions . There exist routines for the easy computation of such a determinant . However , the use of this criterion is optional since its application does not necessarily imply a considerable reduction in the overall

amount of computations required . When one of the polynomials has the form $1 + x^n$ the computation of this determinant can be shortened .

3 . 8 . SOME USEFUL DETAILS .

In the following we discuss some details which may be proven quite useful in certain special cases .

(i) All irreducible factors of $x^{2^n} + x + 1$ have degrees dividing $2n$ and therefore periods dividing $2^{2n} - 1$.

(ii) All irreducible factors of $x^{2^n+1} + x + 1$ have degrees dividing $3n$, therefore periods dividing $2^{3n} - 1$.

Both the above results are given by GOLOMB [4]. In the context of the suggested approach to the factorization problem of polynomials over GF (2) , these results can be used when we encounter a trinomial of the form described in (i) or (ii) after the first step of the suggested algorithm . More specifically they can be used as criteria in order to avoid some unecessary computations . If the number of divisors of n is reasonably small we have to compute only the g. c. d' s between the trinomial and the respective binomials $1 + x^{2^i - 1}$, where i has to

be a divisor of $2n$.

(iii) A polynomial over GF (2) with an even number of terms has $1 + x$ as a factor .

This is a well known result and its proof is obvious . It is an easily applicable criterion for the divisibility of a polynomial by $1 + x$ and therefore we are not required to compute any g. c. d 's for the removal of first degree factors .

(iv) The transformation : $f(x) \rightarrow f(x + 1) = \bar{f}(x)$ leaves the degrees of the irreducible factors of $f(x)$ unchanged , but it may change their exponents .

This is quite interesting in the context of the suggested method , because the application of such a transformation may separate irreducible factors of the same degree and exponent . Therefore the fourth step will be unecessary . For example in the case of $D_i(x) = (1 + x^3 + x^4) (1 + x + x^4)$ both factors of $D_i(x)$ are of degree 4 and exponent 15 . However if we apply the previously mentioned transformation we have :

$$\bar{D}_i(x) = D_i(x + 1) = (1 + (1+x)^3 + (1+x)^4) (1 + (1+x) + (1+x)^4) =$$

$$= (1 + x + x^2 + x^3 + x^4) (1 + x + x^4)$$

But the two factors of $\bar{D}_i(x)$ belong to different exponents namely $1 + x + x^2 + x^3 + x^4$ belongs to the exponent 5 while $1 + x + x^4$ to 15 . Therefore we can factorize $\bar{D}_i(x)$ instead of $D_i(x)$, then apply the inverse transformation on the two factors and find the factors of the original $D_i(x)$. Since we work over GF (2) the inverse transformation is again of the form :

$\bar{f}(x) \rightarrow \bar{f}(x+1) = f(x)$

(v) An interesting result due to Seguin [28], dealing with irreducible factors of degrees which are multiples of 4 , is the following :

Let $p_1, p_2, \ldots, p_r$ be all primes such that :

(i) $p_i \equiv 1 \mod 4$

(ii) 2 is primitive in GF (p_i)

If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} > 1$, then the irreducible factors of $1 + x^n$ over GF (2) are all self-reciprocal and the degree of each of its factors , except for $1 + x$, is a multiple of 4 .

A few more useful details have been considered by GOLOMB [4] which apply to various special cases . However , it should be mentioned that when we arrive at the point of the mechanization of the algorithm , the usefulness of these details is questionable .

3. 9. THE ALGORITHM .

First step .

(i) Compute the following sequence of g. c. d. 's .

$$\text{g. c. d. } \{A_o(x) , A_o'(x) \} = [A_1(x)]^{2^{j_1}} ,$$

$$\text{g. c. d. } \{A_1(x) , A_1' (x) \} = [A_2(x)]^{2^{j_2}} ,$$

.....

$$\text{g. c. d. } \{A_k(x) , A_k' (x) \} = 1 .$$

(ii) Write $A_o(x)$ in the form :

$$A_o(x) = B_o(x) [B_1(x)]^{p_1} ..... [B_{k-1}(x)]^{p_1 \cdots p_{k-1}} ,$$

where , $B_i(x) = \dfrac{A_i(x)}{[A_{i+1}(x)]^{p_{i+1}}}$, and $p_i = 2^{j_i}$.

Second step .

(i) Compute the following sequence of g. c. d. 's .

$$\text{g. c. d. } \{B_i(x) , 1+ x^{n_1} \} = C_{i1}(x) \quad , \quad n_1 = 2^1 - 1 ,$$

$$\text{g. c. d. } \{ \frac{B_i(x)}{C_{i1}(x)} , 1 + x^{n_2} \} = C_{i2}(x) \quad , \quad n_2 = 2^2 - 1 ,$$

$$\text{g.c.d.}\ \{\frac{Bi(x)}{C_{i1}(x)\ C_{i2}(x)}\ ,\ 1 + x^{n_3}\ \} = C_{i3}(x)\ ,\quad n_3 = 2^3 - 1\ ,$$

.....

$$\text{g.c.d.}\ \{\frac{Bi(x)}{\prod_j C_{ij}(x)}\ ,\ 1 + x^{n_m}\ \} = 1\ ,\quad n_m = 2^m - 1\ ,$$

for. i = 0, 1, 2, ..., k-1 .

(ii) Write $A_o(x)$ in the form :

$$A_o(x) = [\,D_1(x)\,]^{d_1}\,[\,D_2(x)\,]^{d_2} \ldots . [\,D_s(x)\,]^{d_s}\ ,$$

where each $D_i(x)$ contains irreducible factors of the same degree .

Third step.

(i) Compute the g.c.d.'s between each $D_i(x)$ and the relevant Cyclotomic Polynomials , (see page 36) .

(ii) Write $A_o(x)$ in the form :

$$A_o(x) = [\,E_1(x)\,]^{f_1}\,[\,E_2(x)\,]^{f_2} \ldots . [\,E_r(x)\,]^{f_r}\ ,$$

where each $E_i(x)$ contains irreducible factors of the same degree and exponent .

Fourth step.

If some $E_i(x)$ is still reducible :

(i) Generate the appropriate Galois Field and try each element to determine the roots of $E_i(x)$, (see page 38). Separate the roots of each irreducible factor according to Theorem 1.6. 7.

o r ,

(ii) Try the irreducible factors of the appropriate Cyclotomic Polynomials to determine which of them divide $E_i(x)$.

3. 10. SOME REMARKS ON THE IMPLEMENTATION OF THE ALGORITHM .

Most of the computations involved in the suggested algorithm can be rather easily computerized or perfomed by simple circuitry , involving almost exclusively feedback shift registers over GF(2) . Some details concerning these techniques are discussed briefly in the following .

3. 10. 1. Generation of Galois Fields .

As we have already pointed out , in the case that the factorization is still incomplete after the third step of the algorithm , we may try and locate the roots of the irreducible factors . This task is relatively easy because we know , that each still reducible factor divides some binomial $1 + x^{2^m - 1}$ and therefore all its roots can be found between the elements of $GF(2^m)$.

For generating a Galois Field of $q = 2^m$, elements , we first need a p r i m i t i v e polynomial of degree m over GF(2) . If $p(x) = \Sigma_{i=o}^{m} p_i x^i$ is such a polynomial and $\alpha \in GF(q)$ one of its roots , we have that , $p(\alpha) = \Sigma_{i=o}^{m} p_i \alpha^i = 0$, and $\alpha^m = \Sigma_{i=o}^{m-1} p_i \alpha^i$ (3.10. 1.) . Using the last relation we can generate the cyclic Galois Group of GF(q) , by producing the powers of its primitive element α , i.e.

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha^2$$

.....

$$\alpha^m = \Sigma_{i=0}^{m-1} p_i \alpha^i$$

.....

$$\alpha^q = \alpha^0 = 1$$

GF(q) is isomorphic to a vector space over GF(2) and the vector representation of its elements could be generated by linear combinations of the first m of its elements. For example let us generate $GF(2^3)$ using the primitive polynomial $1 + x + x^3$.

$$\begin{aligned}
\alpha^0 &= 1 &&= 1\ 0\ 0 \\
\alpha^1 &= \alpha &&= 0\ 1\ 0 \\
\alpha^2 &= \alpha^2 &&= 0\ 0\ 1 \\
\alpha^3 &= 1 + \alpha &&= 1\ 1\ 0 \\
\alpha^4 &= \alpha + \alpha^2 &&= 0\ 1\ 1 \\
\alpha^5 &= 1 + \alpha + \alpha^2 &&= 1\ 1\ 1 \\
\alpha^6 &= 1 + \alpha^2 &&= 1\ 0\ 1 \\
\alpha^7 &= 1 &&= 1\ 0\ 0
\end{aligned} \qquad (3.10.2.)$$

The above seven first vectors and the all zero vector form $GF(2^3)$.

The first three vectors can be used as a basis for the corresponding vector space .

Any GF (q) can be generated by a single shift register with its feedback realized according to the chosen primitive m degree polynomial . More specifically the realization for the generation of the Galois field of $q = 2^m - 1$ elements will be the following

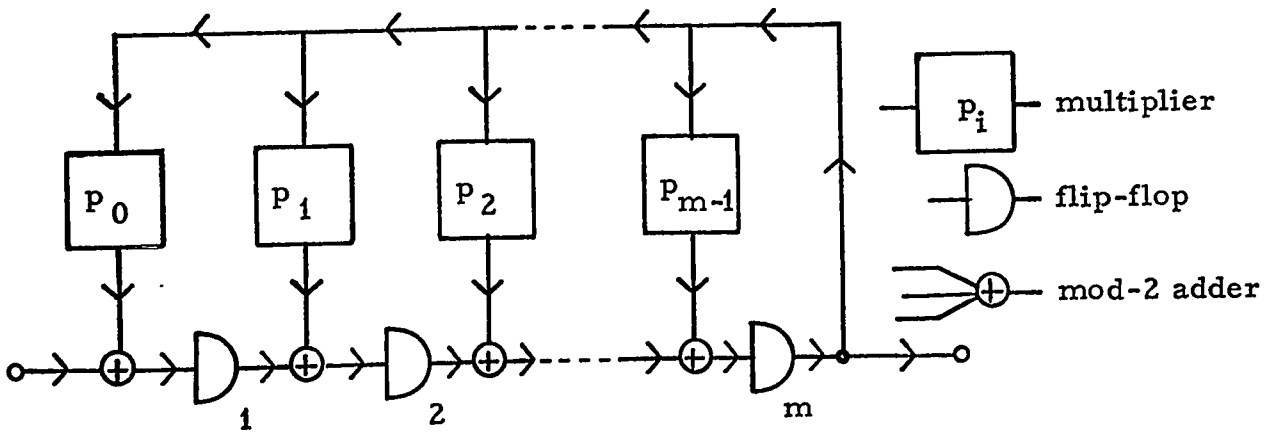

fig . 3. 10. 1.

The multipliers for the GF (2) case are simply connections or no connections depending on the 0 or 1 value of the coefficient p_i of p (x) . The flip-flops are originally all set to zero and a 1 is fed in the first storage element and the contents of all storage elements are shifted q times . After every shift the vector of the contents of the storage elements is the representation of an element of GF (q) appearing in ascending order of powers .

For example the GF (q) in (3. 10. 2.) is generated by the following circuit .

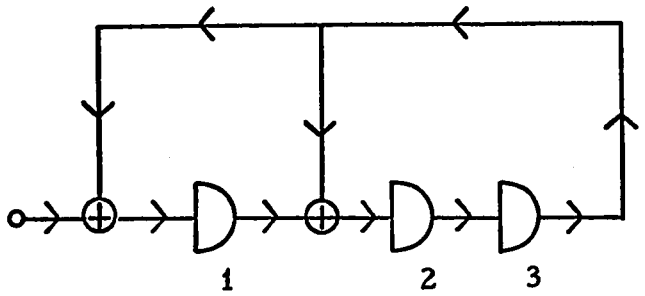

fig . 3. 10. 2.

We should note that a similar shift register realization could be used for counting in a Galois Field , and a more complicated one for multiplying , and raising elements of such fields to given powers .

However these interesting details are beyond the scope of this Chapter ; they are extensively studied in [12, 15, 21, 27]. For the case of testing elements of some Galois Field for locating the roots of a polynomial, we should note that a method similar to Chien 's search [11] could be implemented , which is normally used for the decoding of B C H codes .

A software approach to all the above problems is given in Appendix B .

3. 10. 2. Polynomial Division .

For the computation of the g. c. d. between two polynomials a polynomial division circuit is required . This is also a simple shift register

realization . A circuit dividing polynomials by a fixed polynomial

$g(x) = \Sigma_{i=o}^{r} g_i x^i$ will be of the following type

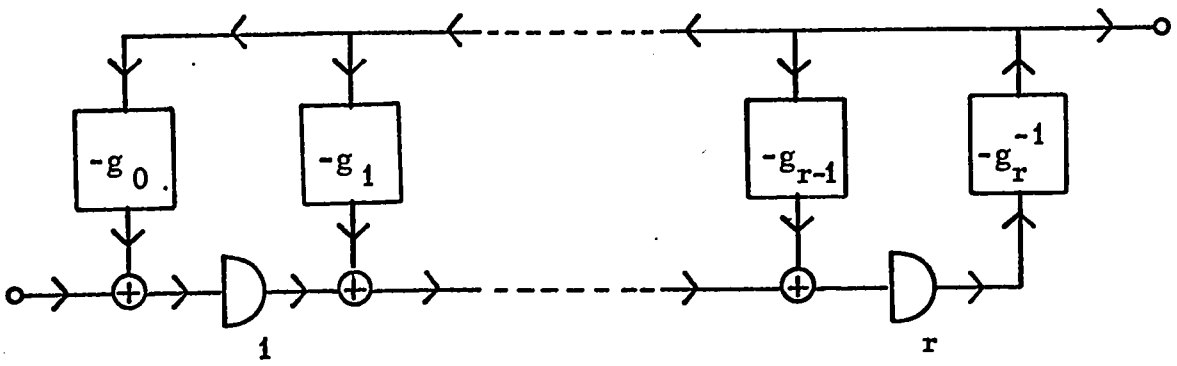

fig . 3. 10. 3.

The storage devices must be set to 0 initially . Then the coefficients of the polynomial $a(x) = \Sigma_{i=o}^{n} a_i x^i$, which we want to divide by $g(x)$, are fed sequentially with a_n coming first . The output is 0 for the first r shifts , then the first coefficient of the quotient appears . After a total of n shifts the quotient has been produced at the output and the remainder is stored in the storage elements .

3. 10. 3. The software approach .

The software approach for the mechanization of the suggested algorithm follows almost the same line with the hardware approach to the problem . Subroutines for polynomial division , the computation of the g. c. d. between two polynomials , the generation of Galois Fields , the computation of formal derivatives of polynomials , the determination

of the roots of polynomials over GF(2) , e. t. c. have been developed . In almost all the cases the polynomials are treated as binary sequences . All the necessary subroutines are given in Appendix B . The following points are significant in the mechanization of the problem .

(i) Step 3 , may be skipped without affecting the final result particularly in the cases of Cyclotomic Polynomials of large number of irreducible factors , (see Table p. 52)

(ii) In Step 4 , the first alternative requires only the knowledge of a primitive polynomial for the generation of the Galois Field , which includes the roots of the polynomial between its elements . The second alternative requires the storage of the irreducible polynomials of a given degree , or the factorization of the related $1 + x^{2^m - 1}$. The application of the first alternative appears to be simpler . However , the necessary computation time increases rapidly with the degree of the irreducible factors of the polynomial .

TABLE I.

Number of irreducible factors of $\psi_i(x)$ over GF(2).

i	deg. $\psi_i(x)$	deg. of irr. fact. of $\psi_i(x)$	Number of irr. fact. of $\psi_i(x)$
1	1	1	1
3	2	2	1
5	4	4	1
7	6	3	2
15	8	4	2
31	30	5	6
9	6	6	1
21	12	6	2
63	36	6	6
127	126	7	18
17	16	8	2
51	32	8	4
85	64	8	8
255	128	8	16
73	72	9	8
511	432	9	48
11	10	10	1
33	20	10	2
93	60	10	6
341	300	10	30
1023	600	10	60
23	22	11	2
89	88	11	8
2047	1936	11	176

CHAPTER IV

CONCLUDING REMARKS.

In the following a comparative review will be attempted between BerleKamp' s algorithm and the approach suggested in Chapter III .

The computations to be performed in Berlekamp' s method may be separated in two classes . First we have the computations involved in the generation of the Q matrix and the required manipulations till a basis of the null-space of the Q - I matrix is found . Second , we have the computations of the Greatest Common Divisors of the form : g.c.d. $\{f(x) , g(x) - s\}$, $s \in GF(q)$, for the one by one separation of the irreducible factors of $f(x)$.

The computations required in the suggested method are almost exclusively computations of Greatest Common Divisors , apart from the last step which is a trial and error procedure . The computations can be divided according to the different steps of the method as described in Chapter III .

4. 1. THE SEPARATION OF MULTIPLE FACTORS .

In Berlekamp' s algorithm no special provision for the multiple factors is considered . They are separated , like any other distinct factor , by the computation of repeated g. c. d. ' s , or by a trial and error procedure , to determine the multiplicity of each separated factor .

However , it appears that it would shorten considerably the total amount of computations , if the first step of the suggested method would be performed independently of the algorithm we have chosen to apply . The first reason is that , although the application of the first step would add the computation of a small number of g. c. d. ' s for the separation of the multiple factors , it would save a much larger number of computations of g. c. d. ' s at the last step of Berlekamp' s algorithm . Because the multiple factors in the first step are separated by groups , but in case that the first step has not been applied the multiple factors should be separated one by one . This fact will be more clear in the next section .

The second reason is that the required matrix manipulations on an nxn matrix are considerably more than the equivalent ones in the case that the nxn matrix has been replaced by a number of square matrices

of dimensions n_1 , n_2 , ... , n_k . Since we have that $n > \Sigma_{i=1}^{k} n_i$, the total number of entries in the second case will be considerably smaller . The first of the previously mentioned reasons is not valid in the case of a polynomial with no repeated factors . However , the cost of the first step will only be the computation of a single g. c. d. equal to 1 indicating the absence of repeated factors . Therefore in the following discussion we shall assume that the polynomial under factorization is either square-free , or that it has been reduced in a product of square-free factors . A similar assumption is made also by McEliece .

In the following we shall attempt to make a rough estimate of the amount of computations required in the different steps of the algorithms . Throughout the algorithms the computation of each g. c. d. is almost always followed by the execution of a polynomial division . Therefore in our discussion , whenever a number of g. c. d. 's will be mentioned , it will be assumed to be followed by an equal number of polynomial divisions . Is also assumed that the polynomial $A_o(x)$ to be factorized , has the following characteristics :

n = number of distinct irreducible factors of $A_o(x)$.

m = degree , of the maximum degree irreducible factor of $A_o(x)$.

l = multiplicity of the maximally repeated factor of $A_o(x)$.

d = degree of $A_o(x)$.

4. 2. COMPUTATIONS IN BERLEKAMP' S METHOD .

We assume that we have already removed the multiple factors of the polynomial to be factorized . The next considerable amount of computations are the matrix manipulations as described in Chapter II , which is proportional to the degree of $A_o(x)$. The next part consists of n - 1 g. c. d.' s to be computed ; since we cannot separate more than one factor every time except the last , where there are only two factors to be separated .

We note that for a polynomial of given degree , the computations of the algorithm are rather independent of the rest characteristics of the polynomial . This is clear for the first step involving the matrix manipulations . The number of g. c. d. ' s to be computed depends on n . However , on the average we should expect an approximately standard number of distinct irreducible factors , for a square-free polynomial of given degree .

4. 3. COMPUTATIONS IN THE SUGGESTED METHOD .

The maximum number of g. c. d. ' s to be computed in the first step

of the suggested method depends on 1 . In general we may say that for an average polynomial , the number of g. c. d. ' s required in the first step is quite small . For example , if n = 8 , k can at most be equal to 3 .

We should note that after k - 1 g. c. d. ' s , k factors of the type $B_i(x)$ result in the first step , because the last g. c. d. separates two factors at the same time .

Since in the second step there are k factors of the type $B_i(x)$, and since we compute the g. c. d. ' s between each of these and each binomial of the form $1 + x^{2^i-1}$, i = 1, 2, ..., m , then at most m.k g. c. d. ' s must be computed . This is again the most unfavorable situation , since we assume that each $B_i(x)$ contains at least one irreducible factor of degree m , and no other bypassing of computations is considered . For example , for some $B_i(x)$ of degree 9 and m = 7, the separation of a factor of degree 4 makes the trials for i= 6 , 7 unecessary . If the computations are monitored , a considerable number of shortcuts of this type , can be made , depending on the characteristics of every particular case . However , if the computations are completely mechanized , it is questionable , if we can take advantage of these cases .

It is clear that the amount of computations in the second step depends mainly on m , since k is a small integer which varies little while m varies considerably .

No meaningful limit can be given for the amount of computations required in the third and fourth step . However , the computations in these two steps are expected to be on the average much less than those in the second step . This is because the probability of meeting factors of the same degree and exponent in the same $B_i(x)$, is rather low . It should be pointed out that , if $A_o(x)$ contains two or more factors of the same degree and exponent , this does not necessarily imply that they cannot be separated without the use of the fourth step . Because the irreducible factors are distributed in the $B_i(x)$ after the first step in a way which depends on the multiplicities of all of them . Such a case is illustrated in example 4 .

4. 4. CONCLUSION .

Berlekamp' s algorithm is a more mathematically elegant solution to the problem of the factorization of polynomials over Finite Fields . The amount of computations required depends almost uniquely on the degree of the given polynomial and is practically standard for an

average polynomial of given degree . The matrix manipulations cannot be reduced for some polynomial of fixed degree , but the number of g. c. d. ' s to be computed would be reduced for the case of polynomials with high degree irreducible factors . Therefore Berlekamp' s algorithm is more efficient in the case of polynomials of high degree irreducible factors , a fact that automatically implies a small n for an average polynomial of given degree . As it has already been mentioned , the separation of multiple factors in the begining , according to the procedure of the first step , is advisable before the application of any algorithm .

The amount of computations in the suggested algorithm is highly dependent on the characteristics of the given polynomial . Particularly important is the value of m . For large values of m the suggested algorithm might be proven time consuming , therefore , Berlekamp' s method should be preferred which , contrary to the above , is more efficient in the cases of large m .

The second weak point of the suggested algorithm is the case where some irreducible factors of the same degree and exponent occur after the third step , in the same $E_{dj}(x)$, and therefore the fourth step is necessary . In such a case m again plays an important role , when the elements of a Galois Field are tested to determine the roots ,

because the number of these elements increases exponentially with m. The probability of reaching the fourth step is quite low, but it cannot be predicted in general before the third step.

However, the suggested method is quite efficient for small values of m. The number of distinct irreducible factors n for a polynomial of given degree, does not affect seriously the total amount of computations. This facts make the suggested algorithm preferable for the cases of large n and small m, where Berlekamp's method appears to be less efficient.

Finally we should point out that at any step of the suggested method we have the alternative to apply Berlekamp's method for any of the reducible factors that have already been separated, if it appears more convenient. The factorization in the first step in particular provides an indication about the values of m and n, providing a basis for the decision about which method should be finally applied.

EXAMPLE 1.

$$A_o(x) = x^{17} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x + 1$$

Step 1.

```
PAS
□   17 14 13 12 11 10 9 8 7 5 4 1 0
 7   5  4  1  0
 5   4  0
TO THE POWER
 2
NO MORE MULTIPLE FACTORS
```

$$A_o(x) = (x^7 + x^5 + x^4 + x + 1) (x^5 + x^4 + 1)^2$$

Step 2.

```
STEP
□   7 5 4 1 0
 2
IRREDUCIBLE
 2  1  0
 5
IRREDUCIBLE
 5  4  3  2  0

STEP
□   5 4 0
 2
IRREDUCIBLE
 2  1  0
 3
IRREDUCIBLE
 3  1  0
```

$$A_o(x) = (x^5 + x^4 + x^3 + x^2 + 1) (x^3 + x + 1)^2 (x^2 + x + 1)^3 .$$

EXAMPLE 2.

$A_o(x) = x^{12} + x^8 + x^7 + x^6 + x^2 + x + 1$

Step 1 .

```
PAS
□    12 8 7 6 2 1 0
NO MORE MULTIPLE FACTORS
```

$\{A_o(x) , A'_o(x)\} = 1$. No repeated factors in $A_o(x)$.

Step 2 .

```
STEP
□    12 8 7 6 2 1 0
 5
IRREDUCIBLE
 5  3  2  1  0
 7
IRREDUCIBLE
 7  5  4  3  0
```

$A_o(x) = (x^7 + x^5 + x^4 + x^3 + 1) (x^5 + x^3 + x^2 + x + 1)$.

EXAMPLE 3 .

$$A_o(x) = x^{13} + x^{12} + x^5 + x^4 + x^2 + x + 1 \ .$$

Step 1

```
PAS
 13 12 5 4 2 1 0
NO MORE MULTIPLE FACTORS
```

g. c. d. $\{ A_o(x) , A'_o(x) \} = 1$. No repeated factors in $A_o(x)$.

Step 2 . .

```
STEP
 13 12 5 4 2 1 0
  4
REDUCIBLE
  8  7  5  4  3  1  0
  5
IRREDUCIBLE
  5  2  0
```

$$A_o(x) = (x^5 + x^2 + 1) (x^8 + x^7 + x^5 + x^4 + x^3 + x + 1)$$

Step 4 .

```
VIMA
 8 7 5 4 3 1 0
 1 1 0 0
THE ROOTS ARE :
 1  2  4  7  8  11  13  14
```

$$(x^8 + x^7 + x^5 + x^4 + x^3 + x + 1) = \{ (x + \alpha) (x + \alpha^2) (x + \alpha^4) (x + \alpha^8) \} .$$

$$\cdot \{ (x + \alpha^7) (x + \alpha^{11}) (x + \alpha^{13}) (x + \alpha^{14}) \} =$$

$$= (x^4 + x + 1) (x^4 + x^3 + 1) \ .$$

$$A_o(x) = (x^5 + x^2 + 1) (x^4 + x + 1) (x^4 + x^3 + 1) \ .$$

EXAMPLE 4 .

$$A_o(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$$

Step 1 .

```
      PAS
□     16 15 14 13 11 9 8 6 4 3 0
 4   3   0
 6   5   4   3   0
TO THE POWER
 2
NO MORE MULTIPLE FACTORS
```

$$A_o(x) = (x^4 + x^3 + 1) (x^6 + x^5 + x^4 + x^3 + 1)^2$$

Step 2 .

```
      STEP
□     4 3 0
 4
IRREDUCIBLE
 4   3   0
      STEP
□     6 5 4 3 0
 2
IRREDUCIBLE
 2   1   0
 4
IRREDUCIBLE
 4   1   0
```

$$A_o(x) = (x^4 + x^3 + 1) (x^4 + x + 1)^2 (x^2 + x + 1)^2 .$$

APPENDIX A .

Proof of Theorem 3. 2. 1.

Let $\alpha_1 , \alpha_2 , \ldots , \alpha_k \in GF(2^q)$, be distinct roots of $f(x)$, of multiplicity $e_1 , e_2 , \ldots , e_k$, respectively . Then $f(x)$ can be written in the form : $f(x) = (x - \alpha_1)^{e_1} (x - \alpha_2)^{e_2} \ldots . (x - \alpha_k)^{e_k}$.

The first formal derivative of $f(x)$ will be :

$$f'(x) = e_1 (x - \alpha_1)^{e_1 - 1} \prod_{j \neq 1}^{k} (x - \alpha_j)^{e_j} + e_2 (x - \alpha_2)^{e_2 - 1} \prod_{j \neq 2}^{k} (x - \alpha_j)^{e_j} +$$

$$+ \ldots\ldots\ldots + e_k (x - \alpha_k)^{e_k - 1} \prod_{j \neq k}^{k} (x - \alpha_j)^{e_j} \quad , \qquad (A1)$$

o r ,

$$f'(x) = \prod_{j=1}^{k} (x - \alpha_j)^{e_j - 1} \{ \sum_{j=1}^{k} \prod_{j=1}^{k} e_j (x - \alpha_j)^{e_j} \} \quad , \qquad (A2)$$

The following two cases are only possible for every α_i :

(i) The respective e_i is even ; then we have $e_i \prod_{j=1} (x - \alpha_j) = 0$, since $GF(2^q)$ has characteristic 2 ; $(x - \alpha_i)$ then , will be a common factor of the remaining terms and therefore α_i will be a root of multiplicity e_i in $f'(x)$.

(ii) The respective e_i is odd ; then $e_i = 1 \bmod 2$, and since all $(x - \alpha_j)$ are distinct , $(x - \alpha_i)$ cannot be a common factor of the

sum in the relation (A2) , therefore a_i will be a root of multiplicity $e_i - 1$.

Q. E. D.

Proof of Theorem 3. 7. 1.

Sufficiency .

Suppose that the value of the determinant is zero . Then there are $I_1(x)$ and $I_2(x)$ such that :

$$P(x)I_1(x) + Q(x)I_2(x) = 0 \ , \qquad (A3)$$

where $I_1(x)$ has degree $q - 1$ or less , and $I_2(x)$ has degree $p - 1$ or less . From (A3) we have , $P(x)\, I_1(x) = Q(x)\, I_2(x)$. but since $I_2(x)$ has degree $p - 1$ or less whereas $P(x)$ has degree p , $\{ P(x) , Q(x) \} = 1$.

Necessity .

Suppose $\{ P(x) , Q(x) \} = 1$. Then $P(x) = G(x)\, P_1(x)$ and $Q(x) = G(x)\, Q_1(x)$. Let us consider $F(x) = P(x)\, I_1'(x) + Q(x)\, I_2'(x) = G(x) \{ P_1(x)\, I_1'(x) + Q_1(x)\, I_2'(x) \}$,

where $I'_1(x)$ has degree $q - 1$ or less and $I_2(x)$ has degree $p - 1$ or less . We also note that $P_1(x)$ has degree $q - 1$ or less . Therefore by making $I'_1(x) = Q_1(x)$ and $I'_2(x) = P_1(x)$, we can make $F(x) = 0$,

that is , the value of the determinant of H is equal to zero .

Q. E. D.

APPENDIX B.

List and description of the utilized APL functions .

P : The vector of the powers of the terms of a polynomial .

S : The binary sequence representation of a polynomial over GF(2) .

1. PAS : First Step .

2. STEP : Second Step .

3. VIMA : Fourth Step (i) , (see page 45) .

4. ROT : Generation of a Galois Field .

   Input : Appropriate primitive polynomial .

   Output : Galois Field in matrix form .

5. FDIV : Polynomial Division .

   Input : In the form S .

   Output : Quotient , in the form S .

6. FREM : Polynomial Division .

   Input : In the form S .

   Output : In the form S .

7. FGCD : Greatest Common Divisor of two polynomials .

   Input : In the form S .

   Output : In the form S.

8. FDIF : Formal derivative of a polynomial over GF(2) .

Input : In the form P .

Output : In the form S .

9. FBIN : Transformation of a polynomial from the form P to the form S .

10. DEC : Transformation of a polynomial from the form S to the form P .

11. BNOM : Generation of binomials of the type $1 + x^n$.

Input : n .

Output : In the form S .

12. EXP : Transformation of a polynomial into the form $[A(x)]^{2^j - 1}$,

(see page 30) .

Input : In the form P .

Output : In the form P .

```
)FNS PAS
```

```
∇ PAS;A;B;C;M;N
 [1] A←⍬
 [2] LOOP:B←FDIF A
 [3] A←FBIN A
 [4] C←A FGCD B
 [5] →((⍴C)=1)/OUT
 [6] A←A FDIV C
 [7] A←DEC A
 [8] A
 [9] M←⍴C
 [10] C←DEC C
 [11] C←EXP C
 [12] C
 [13] N←C[1]
 [14] ' TO THE POWER '
 [15] (M-1)÷N
 [16] A←C
 [17] →LOOP
 [18] OUT: 'NO MORE MULTIPLE FACTORS '
∇
```

```
)FNS STEP
```

```
∇ STEP;A;M;N;K;G;I;Q
 [1] A←⍬
 [2] A←FBIN A
 [3] M←⍴A
 [4] K←I←0
 [5] LOOP:I←I+1
 [6] N←(2*I)-1
 [7] Q←BNOM N
 [8] G←Q FGCD A
 [9] →((⍴G)=1)/LOOP
 [10] A←A FDIV G
 [11] K←K+(⍴G)-1
 [12] I
 [13] →(I=((⍴G)-1))/JUMP
 [14] ' REDUCIBLE '
 [15] →UMP
 [16] JUMP: ' IRREDUCIBLE '
 [17] UMP:G←DEC G
 [18] G
 [19] G←FBIN G
 [20] →(K=(M-1))/0
 [21] →((M-1)>(K+I+1))/LOOP
 [22] (I+1)
 [23] →((I+1)=((⍴A)-1))/LEEP
 [24] ' REDUCIBLE '
 [25] →EEP
 [26] LEEP: ' IRREDUCIBLE '
 [27] EEP:A←DEC A
 [28] A
∇
```

```
)FNS VIMA
```

```
∇ VIMA;POL;K;L;J;P;F;S;D;I
 [1] POL←⍬
 [2] A←⍬
 [3] S←(2*(⍴A))-1
 [4] J←0
 [5] GF←ROT A
 [6] F←(POL[1])⍴0
 [7] D←⍴POL
 [8] K←1
 [9] CYCLE:L←(⍴A)⍴0
[10] P←S|K×POL
[11] I←1
[12] LOOP:→(P[I]=0)/JUMP
[13] L←2|L+GF[P[I];]
[14] →INCR
[15] JUMP:L←2|L+GF[S;]
[16] INCR:I←I+1
[17] →(I≤D)/LOOP
[18] →((L+.=(⍴L)⍴0)=(⍴L))/OUT
[19] BACK:K←K+1
[20] →(K≤S)/CYCLE
[21] →END
[22] OUT:J←J+1
[23] F[J]←K
[24] →BACK
[25] END: ' THE ROOTS ARE : '
[26] F
∇
```

```
)FNS ROT
```

```
∇ W←ROT A;Q;N;I;K
 [1] N←ρA
 [2] Q←Nρ0
 [3] Q[1]←1
 [4] I←0
 [5] K←(2*N)-1
 [6] W←(K,N)ρ0
 [7] LOOP:I←I+1
 [8] →(Q[N]=1)/CYCLE
 [9] Q←¯1φQ
 [10] Q[1]←0
 [11] W[I;]←Q
 [12] →(I=K)/END
 [13] →LOOP
 [14] CYCLE:Q←¯1φQ
 [15] Q[1]←0
 [16] Q←2|Q+A
 [17] W[I;]←Q
 [18] →(I=K)/END
 [19] →LOOP
 [20] END:
∇
```

```
)FNS FDIV
```

```
∇ P←R FDIV W;K;X;Z;O;J
 [1] P←(ρR)ρ0
 [2] K←ρW
 [3] J←0
 [4] LOOP:Z←ρR
 [5] J←J+1
 [6] O←Zρ0
 [7] →(Z<K)/END
 [8] P[J]←Z-K
 [9] W←Zρ W,O
 [10] →((W+.=R)=ρW)/CYCLE
 [11] R←2|R+W
 [12] X←(R⍳1)-1
 [13] R←X↓R
 [14] →LOOP
 [15] CYCLE:R←(ρW)ρO
 [16] END:P←Jρ P
 [17] P← FBIN P
∇
```

```
)FNS FREM
```

```
∇ G←R FREM W;K;Z;O;X
 [1] K←⍴W
 [2] LOOP:Z←⍴R
 [3] O←Z⍴0
 [4] →(Z<K)/END
 [5] W←Z⍴W,O
 [6] →((W+.=R)=⍴W)/CYCLE
 [7] R←2|R+W
 [8] X←(R⍳1)-1
 [9] R←X↓R
 [10] →LOOP
 [11] CYCLE:R←(⍴W)⍴O
 [12] END:G←R
∇
```

```
)FNS DEC
```

```
∇ Q← DEC A
 [1] Q←⍳(⍴A)
 [2] Q←⌽Q
 [3] Q←A×Q
 [4] Q←(Q>0)/Q
 [5] Q←Q-1
∇
```

```
)FNS EXP
```

```
∇ B←EXP A;C
 [1] LOOP:B←A÷2
 [2] C←2|B
 [3] A←B
 [4] →((C+.=((⍴C)⍴0))=⍴C)/LOOP
∇
```

```
)FNS FBIN

∇ P← FBIN F;I
 [1] P←(F[1]+1)ρ0
 [2] I←1
 [3] LOOP:P[(ρP)-F[I]]←1
 [4] I←I+1
 [5] →(I≤ρF)/LOOP
∇

)FNS FDIF

∇ DER← FDIF A;I;B
 [1] I←ρA
 [2] →(A[I]≠0)/JUMP
 [3] A←(I-1)ρA
 [4] JUMP:B←2|A
 [5] A←B/A
 [6] DER←A-1
 [7] DER← FBIN DER
∇

)FNS FGCD

∇ Q←F FGCD H;O;A
 [1] LOOP:A←F FREM H
 [2] O←(ρA)ρ0
 [3] →((A+.=O)=ρA)/OUT
 [4] F←H
 [5] H←A
 [6] →LOOP
 [7] OUT:Q←H
∇

)FNS BNOM

∇ Q← BNOM A
 [1] Q←(A+1)ρ0
 [2] Q[1]←Q[A+1]←1
∇
```

REFERENCES .

[1] E. Berlekamp , " Factoring Polynomials over Finite Fields " , B. S. T. J. , Oct. 1967 , pp. 1853 - 59 .

[2] E. Berlekamp , " Algebraic Coding Theory " , McGraw-Hill Book Co. , N. Y. , 1968 , pp. 74-76 , 87-105 , 146-157 .

[3] R. McEliece , " Factorization of Polynomials over Finite Fields " , Mathematics of Computation , Vol. 23 , No. 108 , pp. 861-867 , Oct. 1969 .

[4] S. W. Golomb , " Shift Register Sequences " , Holden-Day Inc. , San Francisco , Cal. , 1967 , pp. 90-96 .

[5] O. Ore , " On a special class of polynomials " , Trans. Am. Math. Soc. , Vol. 35 , pp. 559-584 , 1933 .

[6] O. Ore , " Contributions to the Theory of Finite Fields " , Trans. Am. Math. Soc. , Vol. 36 , pp. 243-274 , 1934 .

[7] S. G. S. Shiva and P. E. Allard , " A few useful details about a known technique for factoring $1 + x^n$, $n = 2^q - 1$ " , IEEE , Trans. on Inform. Th. , March 1970 .

[8] B. L. Van der Waerden , " Modern Algebra " , Frederick Ungar Publ. Co. , N. Y. , 1940 , pp. 153-163 .

[9] A. A. Albert , " Fundamental Concepts of Higher Algebra " , The Univ. of Chicago Press , 1956 , pp. 37-48 .

[10] G. Birkhoff and S. McLane , " A Survey of Modern Algebra " , The McMillan Co. , N. Y. 1965 , pp. 395-407 .

[11] R. T. Chien , " Cyclic Decoding Procedures for BCH Codes " , IEEE Trans. Inform. Th. , IT10: 357-363 , 1964 .

[12] T. C. Bartee and D. I. Schneider , " Computations with Finite Fields " , Inform. Control , Vol. 6 , pp. 79-98 , 1963 .

[13] R. W. Marsh , " Table of irreducible Polynomials over GF(2) through Degree 19 " , National Security Agency, Washington D. C. , 1957 .

[14] N. Zierler , " On $x^n + x + 1$ over GF(2) " , Inform. Control , Vol. 16 , pp. 502-505 , 1970 .

[15] W. Peterson , " Error Correcting Codes " , The M.I.T. Press , Cambridge , Mass. , 1961 , pp. 11-27 , 87-119 .

[16] G. Seguin , " On the Weight Distribution of Cyclic Codes " , IEEE Trans. Inform. Th. IT16 , May 1970 , p. 358 .

[17] S.E. Tavares , P.E. Allard , S.G.S. Shiva , " Decomposition of Cyclic Codes into Cyclic Classes " , Inform. Control , Vol. 18 , No. 4 , May 1971 , pp. 342-354 .

[18] J. MacWilliams , " The structure and Properties of Binary Cyclic Alphabets " , B.S.T.J. , Vol. 44 , pp. 303-333 .

[19] J.M. Goethals , " Analysis of Weight Distribution in Binary Cyclic Codes " , IEEE Trans. Inform. Th. , Vol. IT12 , pp. 401-402 .

[20] W.S Brown , " ALPAK System for Numerical Algebra on a Digital Computer " , B.S.T.J. , Vol. 42 , Sept. 1963 , pp. 2081-2119 .

[21] H. Tanaka , M. Kasahara , Y. Tezuka , Y. Kasahara , " Computations over Galois Fields using Shift Registers " , Inform. Control , Vol. 13 , 1968 , pp. 75-84 .

[22] G.Birkhoff and T. Bartee , " Modern Applied Algebra " , McGraw-Hill Book Co. , N.Y. 1970 , pp. 359-365 .

[23] H. Paley and P.M. Weichsel , " A first course in Abstract Algebra " , Holt , Reinhart and Winston Inc. N.Y. 1967 , pp. 168-171 .

[24] P.J. McCarthy , " Algebraic Extensions of Fields " , Blaisdell Publ. Co. , 1966 , pp. 1-20 .

[25] N. Jacobson , " Lectures in Abstract Algebra " , 1951 D. Van Norstrand Co. Inc. , Princeton N.J. , pp. 298-300 .

[26] S. Lang , " Linear Algebra " , Addison-Wesley Publ. Co. , Reading Mass. , pp. 26-36 , 1966.

[27] A. Gill , " Linear Sequential Circuits " , McGraw-hill Book Co. , N.Y. 1970 . pp. 139-157 .

[28] G. Seguin , Ph.D Thesis , Notre Dame University , 1971 .

VITAE

NAME	Loukas Komis
PLACE OF BIRTH	Pyrgos , Greece.
DATE OF BIRTH	May 22 , 1943 .
EDUCATION	Secondary : 1 st Lyceum , Athens , Greece .
	University : University of Athens , Athens , Greece , B. Sc .