SOME RESULTS ON FACTORIZATION OF $1 + X^{2^q - 1}$ OVER GF(2) IN REGARD TO ERROR CORRECTING CODES

by

Paul Emile Allard

Submitted in partial fulfilment of the requirements for the degree of Master of Science.

Department of Electrical Engineering,
Faculty of Pure and Applied Science,
The University of Ottawa,
Ottawa, CANADA

January, 1969

ABSTRACT

Some of the methods employed for finding irreducible polynomials over a finite field of 2 elements are considered. Because of their limitations, the possibility of factoring directly the polynomial $1 + x^{2^q-1}$ is explored. Some new theorems are presented which prove most helpful towards this end.

ACKNOWLEDGEMENTS

The author wishes to gratefully acknowledge the assistance provided by Prof. S.G.S. Shiva in the preparation of this work. Thanks are also due to G. Seguin, R. Roy, T. Zeitoun, all former graduate students in the Electrical Engineering Department at the University of Ottawa. Finally, the author is grateful to the National Research Council of Canada, and the University of Ottawa for their financial assistance.

LIST OF SPECIAL SYMBOLS

$a \in A$	:	the element a belongs to the set A.
$A \subseteq B$	:	the set A belongs or is equal to the set B.
$a \mid b$	:	a divides b.
g.c.d.	:	greatest common divisor.
$(m,n)=d$	:	g.c.d. of m and n is d.
$f:R \rightarrow R$	:	the function f that maps R into R.
$\phi_n(x)$	:	n^{th} cyclotomic polynomial.
ϕ	:	Euler ϕ-function.
E	:	finite field with 2^q elements.
F	:	finite field with 2 elements.
$E[x]$	:	polynomial ring with coefficients in E.
u	:	Moibus u-function.
F(a)	:	extension field of F containing a.
Y	:	auto-morphism defined on E.
$T_{E/F}(x)$	:	trace of the element x belonging to E.

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

INTRODUCTION:

The theory of the reducibility of polynomials over a finite field has come to play an increasingly important role in some areas of communication engineering. For instance, irreducible polynomials over a GF(2) occupy a basic position in contemporary linear coding theory, by providing the basis of binary cyclic schemes like BCH codes (1). Also, primitive polynomials provide the logic for generating MLSR (maximum length shift register) sequences (2). This thesis presents a brief survey of some of the methods most commonly employed in finding irreducible polynomials over a finite field of 2 elements. Special emphasis is placed on the role of m-sequences in obtaining irreducible polynomials. A method for obtaining an irreducible polynomial of degree 2m from one of degree m is also given. Finally, the problem of the factorization of the polynomial $1 + x^{2^q-1}$ is considered in detail. As it is well known, every irreducible polynomial of degree r over a GF(2) is a factor of the polynomial $1 + x^{2^q-1}$, where r divides q; and conversely, the irreducible factors of the polynomial $1 + x^{2^q-1}$ over a GF(2) are all the irreducible polynomials of degree r where r divides q (3). In this thesis, some new theorems are presented which further helps in the factorization of the polynomial $1 + x^{2^q-1}$, and as such are most helpful in helping to obtain irreducible polynomials over a GF(2).

CHAPTER I - SOME ALGEBRAIC FUNDAMENTALS

1-1-0 GROUPS

DEFINITION 1-1-1

A group is a non-empty set of elements G together with a binary operation defined on G denoted by (.) and which satisfy the following axioms:

a) the operation is associative i.e. for all a, b, c $\in$ G

$$a.(b.c) = (a.b).c$$

b) there exists an element e $\in$ G such that for all a $\in$ G

$$a.e = a$$

e is called the right identity of G.

c) for all a $\in$ G there exists an element a' such that

$$a.a' = e$$

a' is called the right-inverse of a.

DEFINITION 1-1-2

A group is called commutative or abelian if the additional axiom is satisfied:

d) for all a, b $\in$ G

$$a.b = b.a$$

DEFINITION 1-1-3

Let H be a subset of elements of G. If H is also a group, then H is said to be a subgroup of G.

DEFINITION 1-1-4

$$a^n = \underbrace{a.a.a.....a}_{n}$$

$$a^{-m} = (a^{-1})^m$$

$$a^o = e$$

and it can be shown (4) that the familiar laws on exponents hold

$$a^m.a^n = a^{m+m}$$

$(a^m)^n = a^{mn}$ for all m, n ϵ I (the set of integers)

DEFINITION 1-1-5

The number of elements in a group is called the order of the group denoted by G . The group G is called finite or infinite as it's order is finite or infinite.

DEFINITION 1-1-6

The order of an element a in a group G is the least positive integer m such that $a^m = e$; if no m exists for which $a^m = e$, a has order infinity.

DEFINITION 1-1-7

A group G is said to be cyclic if it contains some one element a whose powers exhaust G; the element a is said to be a generator of the group G.

THEOREM 1-1-8

Let a be an element of a finite group G. Let the order of a be m, then the set of elements generated by the powers of a form a cyclic subgroup of G.

Proof

Since a is an element of G axiom (a) is satisfied. The inverse of a^i is a^j where $i+j=m$, and since $a^m=e$ the set of elements $\left\{ a^k \mid k=0, 1, 2, \ldots m-1 \right\}$ form a cyclic subgroup of G.

DEFINITION 1-1-9

Let G be a group. If $a \in G$ and H is a subgroup of G, we shall call the set $aH=\left\{ ab \mid b \in H \right\}$ a left coset of H and we call the element a, a representative of aH. The set $Ha = \left\{ ba \mid b \in H \right\}$ is called a right coset of H.

LEMMA 1-1-10

If G is finite, each left coset has exactly as many elements as H does.

Proof

For the transformation $b \rightarrow ab$ is one to one and each element of the coset aH is the image of only one element $\in$ H.

LEMMA 1-1-11

Two left coset (right coset) aH, bH are either identical or have no common element.

Proof

Supposing aH and bH have a common element $c=ah' = bh''$, (h', h'' in H), and $a=bh''(h')^{-1}$. Furthermore, it is seen that since $h''(h')^{-1} \in H$ it follows that $aH \subseteq bH$ similarly we can show that $bH \subseteq aH$ and therefore $aH = bH$.

THEOREM 1-1-12

If G is a finite group of order n and H is a subgroup of order m, then $m \mid n$.

Proof

Since the cosets of H are disjoint and each contains as many elements as H then (number of cosets). H = G

Therefore: H = G / (number of cosets).

COROLLARY

Every element of a finite group G has as order a divisor of the order of G.

Proof

Let $a \in G$, then $\left\{a^k \mid k=0, 1, 2, \ldots(m-1)\right\}$ where $a^m=1$, is a cyclic subgroup by theorem 1-1-8 and the conclusion follows from theorem 1-1-12.

THEOREM 1-1-13

Let G be an abelian group and let a, $b \in G$, let the order of a and b be n and m respectively. The order of ab is then m.n if (m, n)= 1.

Proof

Let d be the order of ab

i.e. $(ab)^d = a^d.b^d = 1$

$$a^d = b^{-d}$$

$$a^{nd} = b^{-nd} = 1$$

therefore $m \mid nd$ and $m \mid d$ since $(m, n) = 1$

similarly, $a^{md} = b^{-md} = 1$

therefore, $n = md$ and $n \mid d$ since $(n, m) = 1$

so that $d = mn$

COROLLARY

Let G be an abelian group containing elements a and b, of order m and n respectively. Then there is an element $c \in G$ of order l.c.m(m, n).

Proof

Let $m = p_1^{e_1}.p_2^{e_2}.p_3^{e_3}\ldots p_s^{e_s}$

$$n = p_1^{f_1}.p_2^{f_2}.p_3^{f_3}\ldots p_s^{f_s}$$

where, $p_i^{e_i} < p_i^{f_i}, \qquad 1 \leq i \leq k.$

$$p_j^{f_j} < p_j^{e_j}, \qquad k+1 \leq j \leq s.$$

letting, $m_1 = p_1^{f_1}.p_2^{f_2}\ldots.p_k^{f_k}$

$$n_1 = p_{k+1}^{e_{k+1}}\ldots.p_s^{e_s}$$

the order of $a^{m_1}.b^{n_1}$ is then m_1n_1 = l.c.m(m, n).

1-2-0 RINGS

DEFINITION 1-2-1

A ring is a set of elements R equiped with two laws of composition which we shall call addition and multiplication, such that the following axioms are satisfied:

1 - The elements of R form an abelian group under addition.

2 - Multiplication is associative i.e. for all a, b, c $\in$ R

$a.(b.c) = (a.b).c.$

3 - Multiplication is distributive with respect to addition i.e. for all a, b, c $\in$ R

$a.(b+c) = a.b+a.c$

$(b+c).a = b.a+c.a$

DEFINITION 1-2-2

A ring is commutative if in addition it satisfies the further property that multiplication is commutative i.e. for all a, b $\in$ R

$a.b = b.a$

DEFINITION 1-2-3

A ring is called a ring with identity if it possesses a multiplication identity i.e. for all a $\in$ R,

$a.e = a$

$= e.a$

1-3-0 FIELDS

DEFINITION 1-3-1

A field is a set of elements F on which two operations are defined which we call addition (+) and multiplication (.) and for which the following conditions hold:

1 - the elements of F form an abelian group under addition

2 - the elements of F form an abelian group under multiplication.

1-4-0 VECTOR SPACES

DEFINITION 1-4-1

Let F be a field. A vector space over F is a set V equiped with a law of composition which we shall call addition, and an operation which assigns to every element a of F and every x of V an element of V which we denote by ax, such that the following conditions are satisfied.

1 - The elements of V form an abelian group under the addition operation.

2 - For all a, b of F and all elements x, y of V we have

$(a+b)x = ax+bx$

$a(x+y) = ax+ay$

$a(bx) = (ab)x$

$e(x) = x$ where e is the identity of F.

DEFINITION 1-4-2

Let V be a vector space over a field F. A finite subset $x_1, x_2, \ldots x_k$ of V is said to be linearly dependant over F if there exists elements $a_1, a_2 \ldots a_k$ of F, not all zero, such that $a_1x_1 + \ldots + a_kx_k = 0$.

Otherwise the subset is said to be linearly independant.

DEFINITION 1-4-3

The dimension of a vector space V over a field F is the maximum number of linearly independant elements of V over F.

1-5-0 POLYNOMIALS (5)

DEFINITION 1-5-1

Let R be a ring. A polynomial F over R is a sequence $(a_o, a_1, a_2 \ldots)$ of elements from R in which only a finite number of terms are different from zero.

DEFINITION 1-5-2

Let $a=(a_o, a_1 \ldots, a_n \ldots)$, $b=(b_o, b_1 \ldots . b_n \ldots)$ be two polynomials. Define

$a+b = (a_o+b_o, a_1+b_1, \ldots a_n+b_n \ldots)$ and

$a.b = (c_o, c_1 \ldots c_n \ldots)$.

where $c_k = \sum_{c=o}^{k} a_i \, b_{k-i}$

THEOREM 1-5-3

Let R be a ring with identity 1. Let x denote the polynomial $(0,1,0,0\ldots)$. Then $x^n=(0,0\ldots.0,1,0)$ where 1 appears as the $(n+1)$th term, and any polynomial $(b_0 b_1,\ldots b_k\ldots)$ can be expressed in the form

$$b_0 + b_1x + b_2x^2 + \ldots + b_kx^k.$$

With the notation introduced in theorem 1-5-3 let us denote the set of all polynomials over R by $R[x]$; furthermore, the degree of a polynomial will be defined as the highest power of x, present in the polynomial.

THEOREM 1-5-4

$(R[x],+,\cdot)$ is a ring, called the ring of polynomials over R.

DEFINITION 1-5-5

Let F be a field, $f(x) \in F[x]$, with $f(x)= a_0+a_1x+\ldots+a_nx^n$. We define $f:F\longrightarrow F$ as follows:

Let $s \in F$, then $f(s)= a_0a_1s+\ldots a_ns^n$. The function f is called the polynomial function corresponding to f(x).

DEFINITION 1-5-6

Let $a \in E$ an arbitrary field. If f(x) is a polynomial belonging to $E[x]$ such that $f(a) = 0$, then a is called a root of the polynomial f.

DEFINITION 1-5-7

Let $f(x) \in F[x]$, F a field, deg. $f(x) > 1$. Then $f(x)$ is called irreducible if whenever $h(x) \mid f(x)$, then either $h(x) = c \in F$ or $h(x) = c\, f(x)$, where c is a constant.

DEFINITION 1-5-8

Let $f(x) = a_0 + a_1 x + \ldots a_n x^n$, then $f(x)$ is said to be monic if $a_n = 1$.

DEFINITION 1-5-9

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. The derivative of $f(x)$ is defined to be the polynomial $f' = \sum_{i=1}^{n} i\, a_i x^{i-1}$.

THEOREM 1-5-10

Let $f(x) \in F[x]$. Then f has a multiple root if and only if $(f, f') = 1$.

THEOREM 1-5-11

Let $g(x)$ devide $f(x)$ then every root of $g(x)$ is also a root of $f(x)$.

1-6-0 FIELD EXTENSION

DEFINITION 1-6-1

Let E and F be fields, such that $F \subset E$, then E is said to be an extension of F.

DEFINITION 1-6-2

Let $f(x) \in F[x]$. Then $f(x)$ is said to split in an extension E of F if $f(x)$ can be factored as a product of linear factors in $E[x]$. E is said to be a splitting field for $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E which contains F.

THEOREM 1-6-3

Any two splitting field of $f(x) \in F[x]$ are isomorphic.

DEFINITION 1-6-4

An ideal G is a subset of a ring R with the following two properties:

a) G is a subgroup of the additive group of R.

b) For any element g of G and any element r of R, gr and rg are in G. (This is sometimes called a two-sided ideal).

THEOREM 1-6-5

A set of polynomials is an ideal if and only if it consists of all multiples of some polynomial.

Proof

Let $m(x)$ be the smallest non-zero polynomial in the ideal, and $n(x)$ be any other polynomial in the ideal. Let $d(x)$ be the g.c.d. of $m(x)$ and $n(x)$ and since $d(x) = a(x)\, m(x) + b(x)\, n(x)$, $d(x)$ is also in the ideal by definition, and therefore $m(x) \mid d(x)$. Since $m(x)$ is the smallest polynomial in the ideal

deg (d(x)) $\leq$ deg (m(x)) and since d(x) divides m(x) deg (m(x)) $\leq$ deg (d(x)). Therefore m(x) = d(x) and m(x) devides every polynomial in the ideal.

An ideal generated by a polynomial p(x) will be denoted by $\{ p(x) \}$.

DEFINITION 1-6-6

A residue class is a set of polynomials of the form $a(x) + \{ p(x) \}$ where $a(x) \in F[x]$.

THEOREM 1-6-7

Every residue class modulo a polynomial p(x), of degree n, contains either 0 or a polynomial of degree less than n. Zero is an element of the ideal and every polynomial of degree less than n is in a distinct residue class.

Proof

If s(x) is any element of a residue class, then since

$$s(x) = p(x)q(x) + r(x)$$

r(x) is in the same residue class, and deg (r(x)) $<$ deg (p(x)). If r(x) and s(x) are in the same residue class r(x)-s(x) is an element of the ideal and hence a multiple of p(x). If $r(x) \neq s(x)$, clearly the degree of r(x) and s(x) could not be less than deg (p(x)).

Let $r(x), s(x), p(x) \in F[x]$ and deg (r(x)), deg (a(x)) $<$ deg p(x). Then by theorem 1-6-7, r(x) and s(x) define

two residue class of the form

$$\bar{r}(x) = r(x) + \{ p(x) \}$$
$$\bar{s}(x) = s(x) + \{ p(x) \}$$

We define two operations on these residue classes

a) $\bar{r}(x) + \bar{s}(x) = \overline{r(x) + s(x)}$

b) $\bar{r}(x).\bar{s}(x) = \overline{r(x).s(x)}$

it can be shown (6) that these operations are well defined and that the residue classes form a ring called the residue class ring.

THEOREM 1-6-8

Let F be a field. The polynomial ring F [x] modulo p(x) is a field if and only if p(x) is irreducible.

Proof

If p(x) is not irreducible, then $p(x) = r(x).s(x)$ where r(x) and s(x) define two residue class.

It follows that:

$$r(x)s(x) = 0 \text{ modulo } p(x)$$

and $r^{-1}(x)r(x)s(x) = s(x) = 0$ modulo p(x) a contradiction and therefore r(x) cannot have an inverse and the residue class ring is not a field.

If, however, p(x) is irreducible, then for any residue class m(x), we have

$$a(x)p(x) + b(x)m(x) = 1$$

and $b(x)m(x) = 1$ modulo p(x) and every residue class has an inverse. This field will be denoted by

$$F[x] / \{ p(x) \} .$$

THEOREM 1-6-9

The residue classes of polynomials modulo a polynomial $p(x)$ of degree n forms a vector space of dimension n over the coefficient field.

Proof

It is easily verified that all the axioms for a vector space are satisfied. That it has dimension n can be seen from the fact that the n residue classes, $\overline{1}, \overline{x}, \overline{x^2} \ldots \overline{x^{n-1}}$ span the space, since every residue class contains a polynomial of degree less than n and

$$\overline{a_0 + a_1x + a_2x^2 + \ldots a_{n-1}x^{n-1}} = \overline{a}_0 + \overline{a_1x} + \overline{a_2x^2} + \ldots + \overline{a_{n-1}x^{n-1}}$$

now the left-hand side of the above expression, is zero, only if it is divisible by $p(x)$, which is impossible.

Also if $p(x)$ is irreducible, the residue class form a field $E = F[x] / \{p(x)\}$ and the degree of E over F is n, denoted by $[E:F] = n$.

DEFINITION 1-6-10

An extension $E \supset F$ is called a finite extension of F of degree n, if E is a finite dimensional vector space of dimension n over F.

THEOREM 1-6-11 (7)

If D is a finite extension of E, and E is a finite extension of F, then $[D:F] = [D:E]\,[E:F]$.

THEOREM 1-6-12

Let F be a field. If $p(x)$ is a non-scalar polynomial in $F[x]$, there exists a field $E \supset F$ in which $p(x)$ has a root.

Proof

It clearly suffices to prove this theorem for irreducible polynomials and we now assume that $p(x)$ is irreducible. Let $p(x) = c_0 + c_1x + \ldots + c_nx^n$. From theorem 1-6-8, we know that $E = F[x] / \left\{ p(x) \right\}$ is a field. We shall see that up to isomorphism E satisfies the conclusion of the theorem. That isomorphism begins with the identification of the elements in F with the scalar polynomials in $F[x]$ and it is continued by the natural mapping of the elements of $F[x]$ onto the residue classes of $F[x] / \left\{ p(x) \right\}$ given by $\phi(a(x)) = a(x) + \left\{ p(x) \right\} = \overline{a}(x)$, the residue class of $F[x] / \left\{ p(x) \right\}$ to which $a(x)$ belongs. Since ϕ is a homomorphism:

$$\phi(p(x)) = \phi(c_0 + c_1x + \ldots + c_nx^n) = \phi(c_0) + \phi(c_1x) + \ldots + \phi(c_nx^n)$$
$$= \overline{c}_0 + \overline{c_1x} + \overline{c_2x^2} + \ldots \overline{c_nx^n} = 0$$

so that the polynomial $p(x)$ irreducible over F, now has a zero $\overline{x}$ in $F[x] / \left\{ p(x) \right\}$.

DEFINITION 1-6-13

If F is a subfield of E and if A is an arbitrary set of elements of E, we shall denote by F(A) the smallest subfield containing F and A.

THEOREM 1-6-14 (8)

Let E be an extension of F. Let p(x) be an irreducible polynomial of $F[x]$, and let $a \in E$ be a zero of p(x). Then F(a) is isomorphic to $F[x] / \{p(x)\}$ and if deg (p(x)) = n, then $1, a, a^2, \ldots a^{n-1}$ is a basis for F(a) over F.

THEOREM 1-6-15

Let $f(x) \in F[x]$ have degree n. Let E be an extension of F. If $f(x) = c(x-a_1)(x-a_2)\ldots(x-a_n)$ in $E[x]$, then $F(a_1, a_2, \ldots a_n)$ is a splitting field for f(x) over F.

Proof

f(x) splits in $H = F(a_1, a_2, \ldots a_n)$ since each factor $x-a_i \in H[x]$. Now suppose f(x) splits in K where $F \subseteq K \subseteq E$. In particular $x-a_i \in K[x]$ and so $a_i \in K$ thus $\{a_1, a_2 \ldots a_n\} \subset K$ and so $H \subseteq K$ and we have shown that f(x) can split in no proper subfield of H which contains F.

1-7-0 MINIMUM POLYNOMIAL

DEFINITION 1-7-1

Let b be an element of E, an extension field of F. The monic polynomial $m(x) \in F[x]$, of smallest degree, such that m(b) = 0 is called the minimum polynomial of b.

THEOREM 1-7-2

The minimum polynomial m(x) of any element $b \in E$, is irreducible.

Proof

Suppose, on the contrary:

$$m(x) = m_1(x)m_2(x)$$

$$\text{then } m(b) = m_1(b)m_2(b) = 0$$

and at least one of the factors $m_1(b)$ or $m_2(b)$ must equal zero. However, this contradicts the definition of a minimum polynomial, since deg $(m_1(x))$, deg $(m_2(x))$ $<$ deg $(m(x))$.

THEOREM 1-7-3

If $f(x) \in F[x]$ and is such that $f(b) = 0$, where $b \in E \supset F$, then $f(x)$ is divisible by the minimum polynomial $m(x)$ of b.

Proof

Since by the Eucledian algorithm,

$$f(x) = m(x)q(x) + r(x)$$

where deg $(r(x))$ $<$ deg $(m(x))$

and since $f(b) = m(b)q(b) + r(b) = 0$

it follows that $r(b) = 0$.

THEOREM 1-7-4

Let $p(x)$ be a monic irreducible polynomial such that $p(b) = 0$, for some $b \in E \supset F$. Then $p(x)$ is the minimum polynomial of b.

Proof

Let m(x) be the minimum polynomial of b:

Therefore $p(x) = m(x)q(x) + r(x)$

where deg $(r(x)) <$ deg $(m(x))$

since $p(b) = m(b)q(b) + r(b) = 0$

$r(b) = 0$, and since $p(x)$ is irreducible $q(x) = 1$.

1-8-0 FINITE FIELDS

DEFINITION 1-8-1

A finite field, is a field with a finite number of elements.

THEOREM 1-8-2

Let p be a prime, and n a positive integer. Then there exists a field with p^n elements. Moreover, any two fields with p^n elements are isomorphic.

Proof

Consider the polynomial $xp^n - x$ over the field of integers modulo p, denoted by Ip. Then by theorem 1-6-15, there is a splitting field for $x^{p^n} - x$, given by $E = Ip(a_1, a_2 \ldots a_n)$ where the a_i's are all the roots of $x^{p^n} - x$ in E. We show that E has precisely p^n elements. If a_1 and a_2 are roots of $xp^n - x$, then $(a_1 + a_2)^{p^n} - a_1 + a_2 = a_1^{p^n} + a_2^{p^n} - a_1 - a_2$; since $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ modulo p and $a_1 + a_2$ is a root of $x^{p^n} - x$, also $a_1 - a_2$ is also a root. Assuming $a_1 \neq 0$, we see that $(a_1^{-1})^{p^n} = (a_1^{p^n})^{-1} = a_1^{-1}$, and so a_1^{-1} is also a root of

$x^{p^n} + x$. Thus the set of all solutions of $x^{p^n} - x = 0$, form a subfield of E, and hence equals E, by the definition of a splitting field. If E has fewer than p^n elements, then $x^{p^n} - x$ has a multiple root in E. However, by theorem 1-5-10, $x^{p^n} - x$ has no multiple roots, and E has precisely p^n elements. The uniqueness follows from theorem 1-6-3.

DEFINITION 1-8-3

A field with p^n elements is called a Galois field and is denoted by $GF(p^n)$.

THEOREM 1-8-4

The multiplicative group of $GF(p^n)$ is cyclic.

Proof

We need to prove that the multiplication group of $GF(p^n)$, has an element of order $p^n - 1$ (theorem 1-1-8). By the corollary to theorem 1-1-13, in a finite abelian group G, if a has order r, and b has order s, then there is an element c in G whose order is l.c.m.(r,s). Thus since there is a finite number of elements in the multiplicative group of $GF(p^n)$, there is an element in this group whose order is the l.c.m. of all the orders. Let this order be m'. We consider $x^{m'} - 1$. Since each a $GF(p^n)$ satisfies $x^{m'} - 1$, it must be that $m' = p^n - 1$ by theorem 1-5-10. Thus the multiplicative group is cyclic.

THEOREM 1-8-5 (3)

If H is a subfield of $GF(p^n)$, then H is isomorphic to $GF(p^m)$, where m divides n. Conversely, if m divides n, then there is exactly one subfield with p^m elements.

THEOREM 1-8-6 (3)

Let g(x) be an irreducible polynomial over GF(p) of degree m. Then g(x) divides $x^{p^n} - x$, if and only if m divides n.

THEOREM 1-8-7 (3)

$x^{p^n} - x$ is the product of all monic polynomials p(x) in GF(p)[x] , such that the degree of p(x) divides n.

THEOREM 1-8-8 (3)

Let f(x) be an irreducible polynomial of degree n over GF(p). Let b be a root of f(x) in some extension field. Then $b, b^p, \ldots b^{p^{(n-1)}}$ are all the roots of f(x).

Proof

In a field of characteristic p, $(a + b)^{p^m} = a^{p^m} + b^{p^m}$ for all positive integer m. It follows therefore, that:

$$(f(x))^{p^n} = (f(x^{p^n}))$$

and so, if b is a root of f(x), b^p, b^{p^2} ... $b^{p^{(n-1)}}$ are also roots. To show that these roots are distinct, assume

$$b^{p^i} = b^{p^j} \text{ where } i < j \leq n - 1,$$

then $b^{p^n} = b = b^{p^{n-i+j}}$, and it follows that b is a root of the polynomial $x^{p^{n-i+j}} - x$.

However, the factors of $x^{p^{n-i+j}} - x$ are polynomials whose degrees are $\leq n-i+j$ by theorem 1-8-7. And so, b is also the root of a polynomial of degree smaller than n

contradicting theorem 1-7-4, therefore, all the roots are distinct.

1-9-0 CYCLOTOMIC POLYNOMIALS

DEFINITION 1-9-1

In the polynomial ring $E[x]$, where $E = GF(p^n)$, let w be a generator of the cyclic group of E. We define $\phi_d(x) = \prod (x - w^{k_i})$, where w^{k_i} consists of all those elements, belonging to E, having order d. $\phi_d(x)$ is called the d^{th} cyclotomic polynomial.

THEOREM 1-9-2 (3)

$$\phi_n(x) = \prod_{d|n} (x^d - 1)^{u(n/d)}$$

where, u is the Möbius u-function, defined by:

$$u(0) = 0$$

$$u(1) = 1$$

$$u(n) = 0 \text{ if } p^2 | n \text{ for some prime } p,$$

$$u(n) = (-1)^k \text{ if } n = p_1 \cdot p_2 \cdots p_k$$

THEOREM 1-9-3

$$x^{p^n-1} - 1 = \prod_{d \,|\, p^n-1} \phi_d(x)$$

Proof

Since $\phi_d(x)$ contains as roots, all those elements having order d, and since $d \,|\, p^n-1$, $\phi_d(x)$ divides $x^{p^n-1} - 1$, and the conclusion follows.

DEFINITION 1-9-4

An element a $\in$ GF(p^n), is said to be primitive, if it has order $p^n - 1$.

DEFINITION 1-9-5

An irreducible polynomial over a GF(p) is said to be primitive, if its roots are primitive elements of GF(p^n).

THEOREM 1-9-6

The factors of $\phi_{p^n-1}(x)$ are primitive polynomials of degree n over GF(p).

Proof

Writing $\phi_{p^n-1}(x) = p_1(x).p_2(x)...p_r(x)$, where, $p_i(x)$ is an irreducible polynomial, whose roots have order $p^n - 1$, for i = 1,2,3...r. Let a be a root of $p_i(x)$. From theorem 1-8-8, a, a^p, a^{p^2},...$a^{p^{(n-1)}}$, are all the roots of $p_i(x)$ and therefore, the degree of $p_i(x)$ is n.

COROLLARY

The number of primitive polynomials of degree n, is given by:

$$N = \phi(p^n - 1)/n,$$

where, ϕ is the Euler-ϕ function

1-10-0 TRACE IN A FINITE FIELD

DEFINITION 1-10-1

Let E = GF(q^n), be a finite field extension of F = GF(q), where, $q = p^m$ for some prime p. Let $T_{E/F}$ be a function defined on E, such that if b $\in$ E,

$$T_{E/F}(b) = \sum_{i=0}^{n-1} b^{q^i}, \text{ where, } b^{q^n} = b.$$

THEOREM 1-10-2

Let a and b be two elements of $GF(q^n)$, and let w be a member of $GF(q)$. Then:

1) $T_{E/F}(b) \in GF(q)$

2) $T_{E/F}(a + b) = T_{E/F}(a) + T_{E/F}(b)$

3) $T_{E/F}(w.b) = w.T_{E/F}(b)$.

Proof

1) $(T_{E/F}(b))^2 = (b + b^q + b^{q^2} + \ldots b^{q^{(n-1)}})^2 = T_{E/F}(b)$, and therefore, $T_{E/F}(b)$ GF(q). (This is the reason the notation $T_{E/F}$ is employed, denoting that $T_{E/F}$, is a mapping from E into F.

2) $$T_{E/F}(a + b) = \sum_{i=0}^{n-1} (a + b)^{2^i} = \sum_{i=0}^{n-1} (a^{2^i} + b^{2^i})$$

$$= \sum_{i=0}^{n-1} a^{2^i} + \sum_{i=0}^{n-1} b^{2^i} = T_{E/F}(a) + T_{E/F}(b).$$

3) $$T_{E/F}(w.b) = \sum_{i=0}^{n-1} (w.b)^{2^i} = \sum_{i=0}^{n-1} w^{2^i}.b^{2^i} = \sum_{i=0}^{n-1} w.b^{2^i} = w.T_{E/F}(b).$$

THEOREM 1-10-3 (9)

There exists a basis $w_1, w_2, \ldots w_n$ of $GF(q^n)$ over $GF(q)$, such that:

$$a^i = T_{E/F}(a^{m+i})w_1 + \ldots + T_{E/F}(a^{m+i+n-1})w_n,$$

where, a, is a primitive element of $GF(q^n)$.

THEOREM 1-10-4 (10)

Let $K = GF(q^n)$ be an extension of $E = GF(q^m)$, which in turn, is an extension of $F = GF(q)$. Then:

$$T_{K/F}(x) = T_{E/F}(T_{K/E}(x)), \text{ for all } x \in K.$$

CHAPTER 2

In this chapter, we consider some of the methods used for obtaining irreducible polynomials over a GF(2). The first method we will consider, consists in writing down all the polynomials of the r^{th} degree, and eliminating those that contain factors of degree $\leqslant r/2$. The process of checking for factors is simplified by the following theorems:

THEOREM 2-1-1 (4)

If g(x) divides f(x), then every root of g(x) is also a root of f(x).

THEOREM 2-1-2 (3)

The polynomial $x^{2^q-1} + 1$ contains all those irreducible polynomial over GF(2) of degree m where m divides q.

Theorem 2-1-1 tells us that a necessary condition for f(x) to be irreducible is that f(x) should not have 1 or 0 as roots, i.e., it should contain an odd number of terms, and not be of the form $f(x) = x.g(x)$. Theorem 2-1-2 enables us to check for factors of degree k, where k divides d, and $d \leqslant r/2$, by finding the greatest common divisor of f(x) and $x^{2^d-1} + 1$. We now illustrate the procedure by an example. Suppose we are required to check for the irreducibility of $f(x) = x^7 + x^5 + x^4 + x + 1$. It is immediately observed that 1 and 0 are not roots of f(x). The factors of f(x) must then have degree 2 or 3.

To check for factors of degree 3, we find the g.c.d. of $f(x)$, and $x^{2^3-1} + 1$, and similarly to check for factors of degree 2, we find the g.c.d. of $f(x)$, and $x^{2^2-1} + 1$. We find:

$$\text{g.c.d.}(f(x),\ x^{2^3-1} + 1) = 1$$

$$\text{g.c.d.}(f(x),\ x^{2^2-1} + 1) = x^2 + x + 1.$$

Therefore, $f(x)$ is reducible containing $x^2 + x + 1$ as a factor.

2-2-0

The second method that we consider, for obtaining irreducible polynomials of degree m over a GF(2), depends heavily on the theory of maximal-length shift register sequences, henceforth, referred to simply as m-sequences. Most of the material presented here can be found in various forms in the litterature (11). However, those theorems that are proven here, are included because it is felt that their proofs are somewhat different, and the theorems are important enough to warrant giving them special attention. This section discusses the theory of m-sequences in some detail, and their relationship to irreducible polynomials over GF(x). This leads to the so-called synthetic method of generating irreducible polynomials to be found in the latter parts of this section.

2-2-1 SHIFT REGISTER SEQUENCES

Basically, a shift register is a set of n flip-flops, connected in series, and operating in such a way, that at the arrival of a clock pulse, the content of F_i is shifted to F_{i+1}, fig. 1.

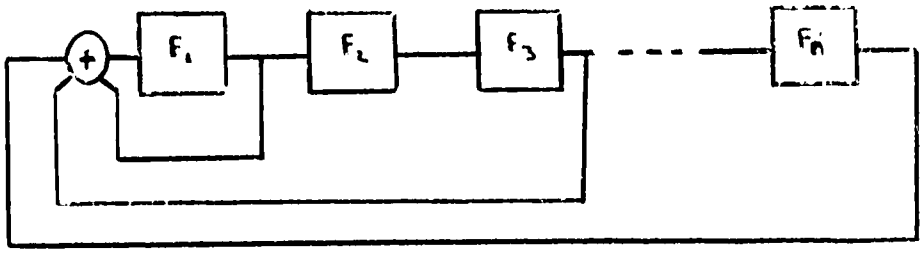

FIG. 1

If there were no feedback, the register would always be empty at the end of the n^{th} pulse. The outputs of some of the flip-flops, are then returned to the first flip-flop via a modulo 2 adder. If an output is taken at any one stage and the register is started in a non-zero state, a sequence of 1 and 0's is observed as the register is pulsed. The same sequence is observed at any stage of the register but either delayed or advanced in time.

THEOREM 2-2-2

The succession of states in a shift register is periodic, with period $p \leq 2^q - 1$, where q is the number of flip-flops.

Proof

Each state of the shift register is completely determined by the previous state. Hence, if it ever happens that a state is the same as some earlier state, then the following

states are also the same, so that a periodicity is established. With a register of q stages, a repetition must occur somewhere amongst the first $2^q + 1$ states. Therefore $p < 2^q$. Finally, if the state "all zeros", ever occurs, the subsequent states will also consist of "all zeros" and the periodicity is 1. Thus, a long period cannot include this state, and $p \leq 2^q - 1$.

DEFINITION 2-2-3

An m-sequence is a shift register sequence having period $2^q - 1$ where, q is the number of stages in the register.

We will now show that there exists feedback connections, which lead to sequences of maximum period. Focussing our attention on the first stage of the register, we will suppose that the history of this stage is given by the successive terms $a_0, a_1 \ldots a_m$. From the feedback arrangement, a_m is a sum, mod 2, of the contents of several of the flip-flops, which themselves represent past states of the first stage. a_m therefore satisfies an equation of the type:

$$a_m = c_1 a_{m-1} + c_2 a_{m-2} + \ldots + c_q a_{m-q},$$

where, the coefficients $c_1, c_2 \ldots c_q$ are all 0 or 1, depending if the feedback path is included, and which do not depend on m.

2-2-4 GENERATING FUNCTION

Given the shift-register sequence $\{a_m\} = \{a_0, a_1 \ldots a_{p-1}\}$, describing the history of the first stage of the register, one may associate with it the generating function

$$G(x) = \sum_{m=0}^{\infty} a_m x^m$$

The initial state of the shift register may be thought of, as being given by, $a_{-1}, a_{-2}, \ldots a_{-q}$. If $\{a_m\}$ satisfies the recurrence relation:

$$a_m = \sum_{i=1}^{q} c_i a_{m-i}$$

$$\text{Then } G(x) = \sum_{m=0}^{\infty} \sum_{i=1}^{q} c_i a_{m-i} x^m = \sum_{i=1}^{q} c_i x^i \sum_{m=0}^{\infty} a_{m-i} x^{m-i}$$

$$= \sum_{i=1}^{q} c_i x^i \left[a_{-i} x^{-i} + \ldots a_{-1} x^{-1} + \sum_{m=0} a_m x^m \right]$$

$$G(x) = \sum_{i=1}^{q} c_i x^i \left[a_{-i} x^{-i} + \ldots a_{-1} x^{-1} + G(x) \right] .$$

Therefore,

$$G(x) = \sum_{i=1}^{q} c_i x^i \left[a_{-i} x^{-i} + \ldots a_{-1} x^{-1} \right] / \left(1 + \sum_{i=1}^{q} c_i x^i\right)$$

This expresses $G(x)$ entirely in terms of the initial conditions $a_{-1}, a_{-2} \ldots a_{-q}$, and the feedback coefficients $c_1, c_2 \ldots c_q$. It will be convenient to refer to the q^{th} degree polynomial $f(x) = 1 + \sum_{i=1}^{q} c_i x^i$ as the characteristic polynomial of the sequences.

THEOREM 2-2-5

If an n stage shift register sequence $\{a_n\}$, obeys the initial conditions $a_{-1} = a_{-2} = \ldots a_{1-n} = 0$, $a_n = 1$, then the period of the sequence is the smallest positive integer p for which the characteristic polynomial $f(x)$ divides

the polynomial $1 + x^p$, mod 2.

Proof

Assuming the sequence to have period p, and under the initial conditions stated:

$$\begin{aligned} G(x) = 1/f(x) &= \sum_{m=0} a_m x^m = (a_0 + a_1 x + \ldots a_{p-1}x^{p-1}) \\ &\quad + x^p(a_0 + a_1 x + \ldots a_{p-1}x^{p-1}) + x^{2p}(a_0 + a_1 x \\ &\quad + \ldots a_{p-1}x^{p-1}) + \ldots\ldots \\ &= (a_0 + a_1 x + \ldots a_{p-1}x^{p-1})(1 + x^p + x^{2p} + \ldots) \\ &= a_0 + a_1 x + \ldots a_{p-1}x^{p-1} \;/\; (1 + x^p). \end{aligned}$$

Therefore,

$f(x)(a_0 + a_1 x + \ldots a_{p-1}x^{p-1}) = 1 + x^p.$

THEOREM 2-2-6

If the sequence $\{ a_m \}$ has maximum period, its characteristic polynomial is irreducible.

Proof

Let f(x) be the characteristic polynomial of the sequence, and suppose:

$$f(x) = s(x).f(x)$$

then

$$1/f(x) = a(x)/s(x) + b(x)/t(x)$$

and, deg $(s(x)) = r_1$

deg $(t(x)) = r_2$

$r_1 + r_2 = q =$ deg $(f(x))$.

Since the period of $a(x)/s(x) \leq 2^{r_1} - 1$, and similarly, since the period of $b(x)/t(x) \leq 2^{r_2} - 1$, it must be that the period of $a(x)/s(x) + b(x)/t(x)$ must satisfy the

relation $$2^q - 1 \leq p \leq (2^{r_1} - 1)(2^{r_2} - 1) \quad 2^q - 3,$$

since this cannot be, f(x) must irreducible. We note that this is a necessary, but not a sufficient condition for maximum period.

THEOREM 2-2-7

If a sequence has an irreducible characteristic polynomial f(x) of degree r, the period of the sequence is a factor of $2^r - 1$.

Proof

By definition:

$$1 + x^p = f(x).m(x),$$

also, from theorem 1-8-7:

$$1 + x^{2^r-1} = f(x).h(x).$$

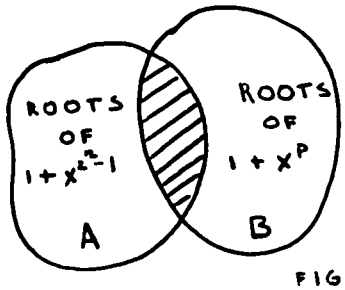

FIG.2

If we can show that all the roots of $1 + x^p$ are also roots of $1 + x^{2^r-1}$, then it will follow that p divides 2^r-1, by Lagrange's theorem. Since the roots of $1 + x^p$ form a cyclic group, consider fig. 2.

The shaded area consists of the roots of f(x) and contains r elements. From theorem 1-8-8, it is clear that the roots of f(x) do not form a group. It is therefore possible to find two roots of f(x) such that their product lie either in A or B. Since this cannot be, B must lie inside A and therefore, p divides 2^r-1.

COROLLARY 1

A necessary and sufficient condition for f(x) to generate a maximum length sequence, is that it be irreducible, and not divide $1 + x^m$ for any $m < 2^r-1$.

Proof

Let f(x) generate a sequence of period p, where p divides 2^r-1, i.e. $pk = 2^r-1$, for some positive integer k.

Therefore, $G(x) = 1/f(x) = \sum_{m=0}^{\infty} a_m x^m$

$$G(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{2^r-1/k}x^{2^r-1/k} + a_0x^{2^r/k} + \ldots\ldots$$

$$= (a_0 + a_1x + \ldots + a_{2^r-1/k}x^{2^r-1/k})(1 + x^{2^r-1/k} + x^{2(2^r-1/k)} \ldots$$

And, $(a_0 + a_1x + \ldots + a_{2^r-1/k}x^{2^r-1/k}) = 1 + x^{2^r-1/k}/f(x)$,

and for maximum period, $k = 1$.

CORROLLARY 2

If 2^r-1 is a prime, every irreducible polynomial of degree r, corresponds to a shift register sequence of maximum length.

CORROLLORY 3

To every m-sequence there corresponds an irreducible polynomial.

With every irreducible polynomial, we can then associate one and only one maximum length sequence, and conversely with every maximum length sequence, we can associate one and only one irreducible polynomial. We will now use this fact for obtaining irreducible polynomials from m-sequences; however, we need a procedure to construct m-sequences which does not involve irreducible polynomials, such a procedure is now developed. To this end, let us then consider some of the properties of the sequence $\left\{T_{E/F}(a^{m+i})\right\}$, where a is a primitive element of $E = GF(2^q)$, an extension of $F = GF(2)$.

THEOREM 2-2-8

The sequence $\left\{T_{E/F}(a^{m+i})\right\}$ is periodic, with periodicity $2^q - 1$.

Proof

This follows readily from the fact that a is a generator of the multiplicative group of $GF(2^q)$. Since the non-zero elements of $GF(2^q)$ form a cyclic group, it follows that the period of $\left\{T_{E/F}(a^{m+i})\right\}$ is $2^q - 1$.

THEOREM 2-2-9

Every q-tuple occurring in the sequence is non-zero, and every non-zero q-tuple occurs exactly once within each period.

Proof

The proof follows from theorem 1-10-3, since under any basis, there is a one-to-one correspondence between the non-zero

element of $GF(2^q)$ and the $2^q - 1$ non-zero q-tuples over $GF(2)$.

It will now be shown, that every m-sequence can be derived as a sequence of the form $\left\{T(a^{m+i})\right\}$. In order to form the m-sequence $\left\{S_i\right\}$, we must be given a primitive polynomial and a non-zero q-tuple over $GF(2)$. Let $f(x) = 1 + c_1x + \ldots + c_{q-1}x^{q-1} + x^q$ be a fixed primitive polynomial, and let $a \in GF(2^q)$ be a zero of $f(x)$. The polynomial $f(x)$ shall be used to generate $\left\{S_i\right\}$ and a shall be used to generate $\left\{T(a^{m+i})\right\}$. Let $S_0, S_1, \ldots S_{q-1}$, be the non-zero q-tuple chosen to start the sequence $\left\{S_i\right\}$. Consider the sequence $\left\{T(a^i)\right\}$. Since every non-zero q-tuple over $GF(2)$ occurs in this sequence, then there is an integer t such that $S_0 = T(a^t)$, $S_1 + T(a^{t+1}) \ldots S_{q-1} = T(a^{t+q-1})$. Let $m = t$, and consider the sequence $T(a^{m+i})$. The first q terms of the sequence are $S_0, S_1, \ldots S_{q-1}$. Now we find the rest of the sequence. Since $f(a) = 0$,

$$a^q + c_{q-1}a^{q-1} + \ldots + 1 = 0 \qquad \ldots(1)$$

multiplying (1) by a^{m+i},

$$a^{m+i+q} + c_{q-1}a^{m+i+q-1} + \ldots a^{m+i} = 0,$$

and therefore,

$$T_{E/F}(a^{m+i+q}) + c_{q-1}\, T_{E/F}(a^{m+i+q-1}) + \ldots + T_{E/F}(a^{m+i}) = 0$$

i.e. $$T(a^{m+i+q}) = c_{q-1}\, T(a^{m+i+q-1}) + \ldots T(a^{m+i}),$$

where, $T = T_{E/F}$.

However, the sequence $\left\{S_i\right\}$ was formed by the rule:

$$S_{i+q} = c_{q-i}S_{i+q-1} + \ldots S_i,$$

and therefore,

$$T(a^{m+q}) = S_q,$$

$$T(a^{m+q+1}) = S_{q+1},$$

etc.

$$\left\{T(a^{m+i})\right\} = \left\{S_i\right\}.$$

The sequence $\left\{T(a^{m+i})\right\}$ is therefore an m-sequence.

THEOREM 2-2-10

Let $S = \left\{S_i\right\}$, $i = 0,1,2,\ldots 2^q - 2$, be an m-sequence. Then, there exists a shift of S such that:

$$S_1 = S_2 = S_4 = \ldots = S_{2(q-1)}$$

$$S_j = S_{2j} = S_{4j} = \ldots = S_{2(q-1)j}$$

for all $j \leq 2^q - 2$, the subscripts being taken mod. $2^q - 1$.

Proof

Let $\left\{S_i\right\} = \left\{T_{E/F}(a^{i+m})\right\}$, $i = 0,1,2,\ldots 2^q - 2$,

and since,

$$T_{E/F}(a^{2^k \cdot i}) = T_{E/F}(a^i),\ k = 1,2,\ldots q - 1$$

where, $2^k.i$, is taken mod. $2^q - 1$; it follows that:

$$S_{i+m} = S_{2(i+m)} = \ldots = S_{2(q-1)(i+m)},$$

and it follows that if $m = 0$

$$S_i = S_{2i} = S_{4i} = \ldots = S_{2(q-1)(i)},$$

where, again the subscripts are taken mod. $2^q - 1$.

LEMMA 2-2-11

Let p be a positive integer. Let 0 n p, be also a positive integer. The set of n such that (n,p) = 1, form an abelian group. There are $\emptyset(p)$ of them, where $\emptyset$ is the Euler-$\emptyset$ function.

LEMMA 2-2-12

If $p = 2^q - 1$, the numbers $1,2,4,8,\ldots 2^{(q-1)}$, form a subgroup modulo p under multiplication.

The numbers from 1 to p-1, can then be written in a table form as indicated below:

$$\text{mod. } 2^q - 1 \qquad \begin{array}{cccc} 1 & 2 & 4 \ldots & 2^{(q-1)} \\ k_1 & 2k_1 & 4k_1 \ldots & 2^{(q-1)}k_1 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ k_n & 2k_n & 4k_n \ldots & 2^{(q-1)}k_n \\ g_1 & 2g_1 & 4g_1 \ldots & 2^{(q-1)}g_1 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ g_m & 2g_m & 4g_m \ldots & 2^{(q-1)}g_m \end{array}$$

where, $(k_i, 2^q-1) = 1$, for $i = 1,2,\ldots n$

$(g_j, 2^q-1) = d \neq 1$, for $j = 1,2,\ldots m$.

The first n + 1 rows are proper cosets, and the last m rows are improper cosets. We note in passing, that the rows consisting of the improper cosets need not contain the same number of elements as the rows containing the proper cosets.

LEMMA 2-2-11

Let p be a positive integer. Let 0 n p, be also a positive integer. The set of n such that (n,p) = 1, form an abelian group. There are $\phi(p)$ of them, where ϕ is the Euler-ϕ function.

LEMMA 2-2-12

If $p = 2^q - 1$, the numbers $1,2,4,8,\ldots 2^{(q-1)}$, form a subgroup modulo p under multiplication.

The numbers from 1 to p-1, can then be written in a table form as indicated below:

$$\text{mod. } 2^q - 1 \qquad \begin{array}{cccc} 1 & 2 & 4 \ldots & 2^{(q-1)} \\ k_1 & 2k_1 & 4k_1 \ldots & 2^{(q-1)}k_1 \\ \ldots & \ldots & \ldots & \ldots \\ k_n & 2k_n & 4k_n \ldots & 2^{(q-1)}k_n \\ g_1 & 2g_1 & 4g_1 \ldots & 2^{(q-1)}g_1 \\ \ldots & \ldots & \ldots & \ldots \\ g_m & 2g_m & 4g_m \ldots & 2^{(q-1)}g_m \end{array}$$

where, $(k_i, 2^q-1) = 1$, for $i = 1,2,\ldots n$

$(g_j, 2^q-1) = d \neq 1$, for $j = 1,2,\ldots m$.

The first n + 1 rows are proper cosets, and the last m rows are improper cosets. We note in passing, that the rows consisting of the improper cosets need not contain the same number of elements as the rows containing the proper cosets.

If we identify the elements in the rows of the table of cosets to the subscripts of the elements of an m-sequence $\left\{ S_i \right\}$, $i = 0,1,2,\ldots 2^q - 1$, then by theorem 2-2-10, the problem is then to make a proper assignment of 1's and 0's to the cosets. Once a proper assignment is made, it becomes possible to find the generating irreducible polynomial of the sequence. As an example, let us construct an m-sequence of period $p = 2^5 - 1$. We first list the cosets:

C_0 : 1 2 4 8 16

C_1 : 3 6 12 24 17

C_2 : 9 18 5 10 20

C_3 : 27 23 15 30 29

C_4 : 19 7 14 28 25

C_5 : 26 21 11 22 13

We then form the products:

$$C_0C_1 = C_0 + C_2 + C_5$$

$$C_0C_2 = C_1 + C_3 + C_4$$

$$C_0C_3 = 1 + C_0 + C_1 + C_3 + C_4$$

$$C_0C_4 = C_0 + C_2 + C_5$$

$$C_0C_5 = C_1 + C_4 + C_5$$

$$C_0C_0 = C_0$$

Where $C_iC_g = \sum (u_i+v_j)$ and, $u_i \in C_i$, $v_j \in C_j$.

We then take $C_0 = 0$, and the set of equations becomes:

$$0 = C_2 + C_5$$
$$0 = C_1 + C_2 + C_4$$
$$0 = 1 + C_1 + C_3 + C_4$$
$$0 = C_1 + C_4 + C_5$$

The set of solutions to the above equations is given below:

	C_0	C_1	C_2	C_3	C_4	C_5
S_1	0	1	0	1	1	0
S_2	0	0	1	0	1	1
S_3	1	0	0	1	0	1
S_4	1	1	0	0	1	0
S_5	0	1	1	0	0	1
S_6	1	0	1	1	0	0

There are then six m-sequence of period $p = 2^5 - 1$ which corresponds to six primitive polynomials of degree 5. Once the sequence is constructed with the help of theorem 2-2-10, the primitive polynomial is found by solving the following set of equations:

$$S_n = C_1S_{n-1} + C_2S_{n\ 2} + \ldots C_4S_{n-4} + S_{n-5}$$

$$S_{n+1} = C_1S_n + C_2S_{n-1} + \ldots C_4S_{n-3} + S_{n-4}$$

.....

Solving for the C's, we then obtain the primitive polynomial of degree 5 which generates the sequence. The foregoing method illustrates the so-called synthetic approach to the construction of irreducible polynomials, while also providing further insight into the actual construction of m-sequences. However, for sequences of large period, the method becomes unmanageable, because of the great number of cosets involved.

2-3-0

In this section, we consider the possibility of obtaining irreducible polynomials from other irreducible polynomials over GF(2). In particular, we discuss a method by which given an irreducible polynomial of degree m over GF(2), which satisfies a very simple condition, we can obtain an irreducible polynomial of degree 2m over GF(2). It is based on the following theorems:

THEOREM 2-3-1 (12)

An element $a \in GF(2^n)$ has zero trace if and only if:

$$a = bY + b,$$

for some $b \in GF(2^n)$, where Y is an automorphism of the form z^{2^i}, for some positive integer i.

THEOREM 2-3-2

The polynomial $x^2 + x + a$ is an irreducible polynomial over $E = GF(2^n)$, where E is an extension field of F = GF(2), if and only if the trace $T_{E/F}(a) = 1$.

Proof

The polynomial $x^2 + x + a$ is reducible in E, if and only if there exists an element $b \in E$ such that:

$$a = b^2 + b,$$

however, a b exists if and only if $T_{E/F}(a) = 0$ by theorem 2-3-1.

2-3-0

In this section, we consider the possibility of obtaining irreducible polynomials from other irreducible polynomials over GF(2). In particular, we discuss a method by which given an irreducible polynomial of degree m over GF(2), which satisfies a very simple condition, we can obtain an irreducible polynomial of degree 2m over GF(2). It is based on the following theorems:

THEOREM 2-3-1 (12)

An element $a \in GF(2^n)$ has zero trace if and only if:

$$a = bY + b,$$

for some $b \in GF(2^n)$, where Y is an automorphism of the form z^{2^i}, for some positive integer i.

THEOREM 2-3-2

The polynomial $x^2 + x + a$ is an irreducible polynomial over $E = GF(2^n)$, where E is an extension field of F = GF(2), if and only if the trace $T_{E/F}(a) = 1$.

Proof

The polynomial $x^2 + x + a$ is reducible in E, if and only if there exists an element $b \in E$ such that:

$$a = b^2 + b,$$

however, a b exists if and only if $T_{E/F}(a) = 0$ by theorem 2-3-1.

THEOREM 2-3-3

Let $f(x)$ be an irreducible polynomial of degree m over $GF(2) = F$,

$$f(x) = 1 + a_1x + a_2x^2 + \dots a_{m-1}x^{m-1} + x^m$$

where, $a_i \in GF(2)$.

If $c \in E$, where E is an extension of F such that $f(c) = 0$, and $T_{E/F}(c) = 1$, then the polynomial $f(x^2 + x)$ is an irreducible polynomial of degree 2m over GF(2).

Proof

Since $T_{E/F}(c) = 1$, the polynomial $x^2 + x + c$ is irreducible over E by theorem 2-3-2, and as such it defines a field H of degree 2 over E, or of degree 2m over F by theorem 1-6-8. If $u \in H$, and $u^2 + u = c$, it follows that u is a root of $f(x^2 + x)$ which is an irreducible polynomial of degree 2m over GF(2).

THEOREM 2-3-4

Let $f(x)$ be an irreducible polynomial of degree n over GF(2), of the form $f(x) = 1 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$, where, $a_i \in GF(2)$. If $c \in E$, where E is an extension of F such that $f(c) = 0$, then $T_{E/F}(c) = a_{n-1}$.

Proof

If c is a root of $f(x)$, then $c^2, c^{2^2}, \dots c^{2^{(n-1)}}$, are also roots by theorem 1-8-8. Now,

$$f(x) = (x - c)(x - c^2)\dots(x - c^{2^{(n-1)}}),$$

$$= 1 + a_1x + \dots + a_{n-1}x^{n-1} + x^n,$$

multiplying out and equating coefficients, we obtain:

$$c + c^2 + c^{2^2} + \ldots + c^{2^{(n-1)}} = a_{n-1} = T_{E/F}(c).$$

We can now outline a procedure for obtaining an irreducible polynomial over GF(2) of degree 2m from an irreducible polynomial over GF(2) of degree m. First, select a primitive polynomial over GF(2) of degree m, and of the form:

$$f(x) = 1 + a_1 x + \ldots + a_{m-2} x^{m-2} + x^{m-1} + x^m.$$

This polynomial defines a field of 2^m elements; furthermore, if c is an element of this field such that $f(c) = 0$, then by theorem 2-3-4 $T_{E/F}(c) = 1$. Also, theorem 2-3-2, the polynomial $x^2 + x + c$ is irreducible over the $GF(2^m)$, and by theorem 2-3-3, $f(x^2 + x)$ is then a polynomial of degree 2m, which is irreducible over GF(2). We illustrate the procedure with a few examples.

EXAMPLE 1

To obtain an irreducible polynomial of degree 4, we use the primitive polynomial $x^2 + x + 1$ over GF(2), and $(x^2 + x)^2 + (x^2 + x) + 1 = x^4 + x + 1$, is an irreducible polynomial of degree 4.

EXAMPLE 2

To obtain an irreducible polynomial of degree 8, we use the primitive polynomial $x^4 + x^3 + 1$ over GF(2), and $(x^2 + x)^4 + (x^2 + x)^3 + 1 = x^8 + x^6 + x^5 + x^3 + 1$, which is an irreducible polynomial of degree 8 over GF(2).

EXAMPLE 3

To find an irreducible polynomial of degree 16, we use the primitive polynomial $x^8 + x^7 + x^2 + x + 1$ over GF(2), and $(x^2 + x)^8 + (x^2 + x)^7 + (x^2 + x)^2 + (x^2 + x) + 1$,

$= 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^9 + x^{12} + x^{15} + x^{16}$, which is an irreducible polynomial of degree 16 over GF(2).

In addition, there exists other well known theorems (12), by which it is possible to obtain irreducible polynomials from other irreducible polynomials over $GF(p^n)$. These are briefly described below:

1) If $f(x) = \sum_{n=0}^{r} a_n x^n$ is irreducible, then

$g(x) = \sum_{n=0}^{r} a_n x^{r-n}$, is also irreducible.

2) If f(x) is irreducible, so is h(x) = f(x+1).

3) If $f(x) = \sum_{n=0}^{r} a_n x^n$ is primitive, then

$g(x) = \sum_{n=0}^{r} a_n x^{2^n-1}$ is also irreducible.

EXAMPLE 3

To find an irreducible polynomial of degree 16, we use the primitive polynomial $x^8 + x^7 + x^2 + x + 1$ over GF(2), and $(x^2 + x)^8 + (x^2 + x)^7 + (x^2 + x)^2 + (x^2 + x) + 1$,

$= 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^9 + x^{12} + x^{15} + x^{16}$, which is an irreducible polynomial of degree 16 over GF(2).

In addition, there exists other well known theorems (12), by which it is possible to obtain irreducible polynomials from other irreducible polynomials over $GF(p^n)$. These are briefly described below:

1) If $f(x) = \sum_{n=0}^{r} a_n x^n$ is irreducible, then

$g(x) = \sum_{n=0}^{r} a_n x^{r-n}$, is also irreducible.

2) If f(x) is irreducible, so is h(x) = f(x+1).

3) If $f(x) = \sum_{n=0}^{r} a_n x^n$ is primitive, then

$g(x) = \sum_{n=0}^{r} a_n x^{2^n - 1}$ is also irreducible.

CHAPTER 3

3-0-0

The methods discussed in chapter 2 for obtaining irreducible polynomials over GF(2), lack either in simplicity or generality. The synthetic method becomes impossible to use for polynomials of high degree, and the methods used for obtaining irreducible polynomials from other irreducible polynomials lack in generality. We therefore consider the possibility of obtaining irreducible polynomials over GF(2) by direct factorization of the polynomial $1 + x^{2^q-1}$. As was already pointed out in chapter 1, the polynomial $1 + x^{2^q-1}$ can readily be factored into its cyclotomic polynomials. In this chapter, some new factorization theorems for the polynomial $1 + x^{2^q-1}$ are presented, which prove to be quite helpful in obtaining irreducible polynomials over GF(2).

3-1 NORM AND TRACE OVER A FINITE FIELD.

THEOREM 3-1-1 (15)

Let F be a finite field with $q = p^m$ elements, p being a positive prime, E an extension of degree n over F which contains F. Then the Galois group of E over F is cyclic, of order n, and is generated by the F-automorphism Y, defined by setting $Y(x) = x^q$ for all element x of E.

DEFINITION 3-1-2

Let E and F be the same as in theorem 3-1-1; we define two mappings $N_{E/F}$ and $T_{E/F}$ of E into F, by setting for every element x of E:

$$N_{E/F}(x) = \prod_{i=1}^{n} Y_i(x)$$

$$T_{E/F}(x) = \sum_{i=1}^{n} Y_i(x)$$

We call $N_{E/F}(x)$ and $T_{E/F}(x)$ the norm and the trace respectively of x from E to F.

THEOREM 3-1-3 (16)

The mapping $N_{E/F}(x)$ is a homomorphism of the multiplicative group of E into the multiplicative group of F; the mapping $T_{E/F}(x)$ is a non-zero homomorphism of the additive group of E into the additive group of F.

THEOREM 3-1-4 (16)

Let D be a finite field which is an extension of F. Let E be a subfield of D containing F. Then, for every element x of D:

$$N_{E/F}(N_{D/E}(x)) = N_{D/F}(x),$$

and $$T_{E/F}(T_{D/E}(x)) = T_{D/F}(x).$$

3-2 RECIPRCCAL POLYNOMIAL

DEFINITION 3-2-1

If f(x) is a polynomial of degree m, and of the form

$$f(x) = 1 + a_1x + a_2x^2 + \ldots + a_{m-1}x^{m-1} + x^m,$$

then the reciprocal f*(x) of f(x) is a polynomial given by:

$$f^*(x) = x^m f(1/x)$$

REMARK 3-2-2

A polynomial is self-reciprocal, if and only if,

$$f(x) = f^*(x).$$

REMARK 3-2-3

If f(x) is a factor of $1 + x^n$, then f*(x) is also a factor since $1 + x^n$ is self-reciprocal.

REMARK 3-2-4

If two polynomials are reciprocals, then the g.c.d. (greatest common divisor) of these must be self-reciprocal.

REMARK 3-2-5

If f(x) is a primitive polynomial, then f*(x) is also primitive.

3-3 PROPER AND IMPROPER COSETS

LEMMA 3-3-1

Let n be a positive integer. The set of numbers m_i, where $0 < m_i < n$ such that g.c.d.$(m_i,n) = 1$, form an abelian group under multiplication. There are $\phi(n)$ of them, where ϕ is the Euler-ϕ function.

LEMMA 3-3-2

If $n = 2^q - 1$, the numbers $1,2,4,8,\ldots 2^{(q-1)}$, form a subgroup modulo n under multiplication.

The numbers from 1 to n-1 can then be written in table form as shown below:

$$
\begin{array}{llll}
1 & 2 & 4 \ldots\ldots & 2^{(q-1)} \\
K_1 & 2K_1 & 4K_1 \ldots\ldots & 2^{(q-1)}K_1 \\
\cdots & \cdots & \cdots & \cdots \\
K_i & 2K_i & 4K_i \ldots\ldots & 2^{(q-1)}K_i \qquad \text{mod. } 2^q-1 \\
L_1 & 2L_1 & 4L_1 \ldots\ldots & \\
\cdots & \cdots & \cdots & \\
L_j & 2L_j & 4L_j \ldots\ldots &
\end{array}
$$

where, $(K_p, 2^q-1) = 1$ for $p = 1,2,\ldots i$

$(L_r, 2^q-1) = d$ for $r = 1,2,\ldots j$, where d is a positive integer.

The first i + 1 rows are called proper cosets, and the last j rows are improper cosets.

DEFINITION 3-3-3

The smallest element in every row of the table is called the coset leader. It must therefore be that the coset leader is always odd.

3-4 SOME KNOWN THEOREMS ON THE FACTORIZATION OF TRINOMIALS OVER GF(2).

THEOREM 3-4-1 (11)

A trinomial over GF(2) not divisible by x, has a repeated factor, if and only if the trinomial is a perfect square.

THEOREM 3-4-2 (11)

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

THEOREM 3-4-3 (11)

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

3-5 FACTORIZATION OF THE POLYNOMIAL $1 + x^{2^q-1}$

LEMMA 3-5-1

Let $E = GF(2^q)$ be an extension of $F = GF(2)$. The trace of every element $x \in E$ from E to F will be either 1 or 0.

Proof

The proof follows directly from the fact that:

$$(T_{E/F}(x))^2 = T_{E/F}(x)$$

and consequently, $T_{E/F}(x) \in F$.

COROLLARY 3-5-2

Let $E = GF(2^q)$ be a field extension of degree n over $F = GF(2)$. Then for every $x \in E$,

$$T_{E/F}(x)(1 + T_{E/F}(x)) = 0$$

THEOREM 3-5-3

$$(1 + x^k + x^{2k} + x^{2^{(L-1)}k})(1 + x^k + x^{3k} + x^{7k} + \ldots x^{(2^{(L-1)}-1)k}) = g(x)(1 + x^{2^q-1})$$

where L and k are positive integers, k being a coset leader such that $x^{2^i k}$ is taken mod. $x^{2^q-1} + 1$ for $i = 0,1,2,\ldots(L-1)$, and $L < n$ such that $2^L k \equiv k \bmod. 2^q - 1$.

Proof

The left-hand side of the above expression is recognized as being equal to:

$$(1 + T_{E/F}(x^k)).(T_{E/F}(x^k))/x^k \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

and since every element of $E = GF(2^q)$, is a root of (1), the right-hand side follows.

COROLLARY 3-5-4

$$(1 + x^{2^q-1}) = (1 + x + x^2 + \ldots x^{2^{(q-1)}})(1 + x + x^3 + \ldots x^{2^{(q-1)}-1})$$

this expression follows from theorem 3-5-3 by letting $k = 1$.

CORROLLARY 3-5-5

$$1 + x^{2^q-1} = (x^{2^{(q-1)}} + x^{2^{(q-1)}-2^0} + x^{2^{(q-1)}-2} + \ldots + 1).$$
$$(x^{2^{(q-1)}-2^0} + x^{2^{(q-1)}-2} + \ldots + 1).$$

This expression is the result of taking the reciprocal polynomials in corollary 1.

COROLLARY 3-5-6

Let k be a positive integer of the form $k = (2^q-1)/(2^r-1)$, for some positive integer r, then:

$$1 + x^{2^q-1} = (1 + x^k + x^{2k} + \ldots + x^{2^{(r-1)}k})(1 + x^k + x^{3k} + \ldots + x^{(2^{(r-1)}-1)k}).$$

Substitution of $k = (2^q-1)/(2^r-1)$ in theorem 3-5-3 will produce the above expression.

THEOREM 3-5-7

In the expression,

$$(1 + x^k + x^{2k} + \ldots + x^{2^{(L-1)}k})(1 + x^k + x^{3k} + \ldots + x^{(2^{(L-1)}-1)k})$$

$$= g(x)(1 + x^{2^q-1}), \text{ of theorem 3-5-3,}$$

$$g(x) = D(x^k + x^{2k} + \ldots x^{2^{(L-1)}k})/x^{(k-1)} \text{ mod. 2,}$$

where D is the derivative operator.

Proof

Let $n = 2^q - 1$, and

$$P_1(x) = 1 + x^k + x^{2k} + x^{4k} + \ldots + x^{2^{(L-1)}k}$$

$$P_2(x) = 1 + x^k + x^{3k} + x^{7k} + \ldots + x^{(2^{(L-1)}-1)k}$$

Then,

$$P_1(x).x^kP_2(x) = x^k\, g(x).(1 + x^n) \quad \ldots\ldots\ldots\ldots\ldots(1)$$

taking the derivative on both sides of (1),

$$D(P_1(x))(x^kP_2(x)) + P_1(x)(D(x^kP_2(x))$$

$$= x^k(1 + x^n)D(g(x)) + g(x)D(x^k(1 + x^n)),$$

furthermore, $D(P_1(x)) = D(x^kP_2(x))$

therefore:

$$D(P_1(x))(P_1(x) + x^kP_2(x)) =$$

$$= x^k(1 + x^n)D(g(x) + g(x)D(x^k(1 + x^n)) \ldots\ldots\ldots(2)$$

taking eq. (2) mod. 2, and remembering that both k and n are odd, and since

$$P_1(x) + x^k P_2(x) = 1 \mod 2,$$

we have $D(P_1(x)) = x^k(1 + x^n)D(g(x)) + g(x)x^{k-1}$,

furthermore, since $D(P_1(x)) < n$, $D(g(x)) = 0$ mod. 2,

i.e. g(x) must contain only even powers of x, so that:

$$g(x) = D(P_1(x))/(x^{k-1}).$$

EXAMPLE 1

$$x^{2^6-1} + 1 = x^{63} + 1$$

Proceeding in accordance with section 3-3, a table of cosets is formed, consisting of both the proper and improper cosets to the subgroup $\{1, 2, 4, 8, 16, 32\}$ mod. 63. By theorems 3-5-3 and 3-5-7 the polynomial corresponding to this coset is written down immediately, at the bottom of the coset, as illustrated below:

$$\begin{matrix} 1 & 2 & 4 & 8 & 16 & 32 \end{matrix}$$
$$(1 + x + x^2 + x^4 + x^8 + x^{16} + x^{32})(1 + x + x^3 + x^7 + x^{15} + x^{31}) = 1 + x^{63}$$

$$\begin{matrix} 5 & 10 & 20 & 40 & 17 & 34 \end{matrix}$$
$$(1 + x^5 + x^{10} + x^{20} + x^{40} + x^{17} + x^{34})(1 + x^5 + x^{15} + x^{35} + x^{12} + x^{29}) = (1 + x^{12})(1 + x^{63}$$

$$(1 + x^{11} + x^{22} + x^{44} + x^{25} + x^{50} + x^{37})(1 + x^{11} + x^{33} + x^{11} + x^{37} + x^{26}) = (1 + x^{14} + x^{26})(1 + x^{63})$$

$$(1 + x^{13} + x^{26} + x^{52} + x^{41} + x^{19} + x^{38})(1 + x^{13} + x^{39} + x^{28} + x^{6} + x^{25}) = (1 + x^{6} + x^{28})(1 + x^{63})$$

$$(1 + x^{23} + x^{46} + x^{29} + x^{58} + x^{53} + x^{43})(1 + x^{23} + x^{6} + x^{35} + x^{30} + x^{20}) = (1 + x^{6} + x^{30} + x^{20})(1 + x^{63})$$

$$(1 + x^{31} + x^{62} + x^{61} + x^{59} + x^{55} + x^{47})(1 + x^{31} + x^{30} + x^{28} + x^{24} + x^{16}) = (1 + x^{30} + x^{28} + x^{24} + x^{16})(1 + x^{63})$$

$$(1 + x^{3} + x^{6} + x^{12} + x^{24} + x^{48} + x^{33})(1 + x^{3} + x^{9} + x^{21} + x^{45} + x^{30}) = (1 + x^{30})(1 + x^{63})$$

$$(1 + x^{15} + x^{30} + x^{60} + x^{57} + x^{51} + x^{39})(1 + x^{15} + x^{45} + x^{42} + x^{36} + x^{24}) = (1 + x^{42} + x^{26} + x^{24})(1 + x^{63})$$

$$(1 + x^{9} + x^{18} + x^{36})(1 + x^{9} + x^{27}) = 1 + x^{63}$$

$$(1 + x^{27} + x^{54} + x^{45})(1 + x^{27} + x^{18}) = (1 + x^{18})(1 + x^{63})$$

$$(1 + x^{21} + x^{42})(1 + x^{21}) = 1 + x^{63}$$

It is also possible to factor $1 + x^{63}$ into its cyclotomic polynomials, these are:

$$1 + x^{63} = \Psi_1 . \Psi_3 . \Psi_7 . \Psi_9 . \Psi_{21} . \Psi_{63}$$

these factors can easily be found by theorem 1-9-2 and we have:

$$\begin{aligned} 1 + x^{63} = {} & (1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6) \\ & (1 + x^3 + x^6)(1 + x + x^3 + x^4 + x^6 + x^8 + x^9 + \\ & + x^{10} + x^{12})(1 + x^3 + x^9 + x^{12} + x^{18} + x^{24} + x^{27} + \\ & + x^{30} + x^{36}). \end{aligned}$$

We now prove a theorem which further helps in the factorization of the polynomial $1 + x^{2^q - 1}$, when q is not a prime.

THEOREM 3-5-8

Let $q = u.v$ in the expression $1 + x^{2^q - 1}$, and let

$$A = x + x^{2^u} + x^{2^{2u}} + \ldots + x^{2^{(v-1)u}} = xB,$$

where

$$B = A.x^{-1}$$

then

$$1 + x + x^3 + x^7 + \ldots + x^{2^{(q-1)} - 1} = B(1 + A + A^3 + \ldots + A^{(2^{(u-1)} - 1)})$$

Proof

The proof of this theorem follows directly from theorem 3-1-4 where if D is an extension of E and E is an extension of F then

$$T_{D/F}(x) = T_{E/F}(T_{D/E}(x))$$

THEOREM 3-5-9

Let $q = u.v$ in the expression $1 + x^{2^q-1}$, then

$$x(1 + x^{2^q-1}) = A(1 + A^{2^u-1})$$

where $$A = x + x^{2^u} + x^{2^{2u}} + \ldots + x^{2^{(v-1)u}}.$$

Proof

The roots of the polynomial $x + x^{2^q}$ form a finite field which we call E. Since $q = u.v$, then there exists a subfield having 2^u elements which we call F. Furthermore, the expression

$$x + x^{2^u} + x^{2^{2u}} + \ldots + x^{2^{(v-1)u}}$$

represents the trace of E over F, and as such will map every element of E into F. Since the non-zero elements of F must satisfy the equation $x^{2^u-1} + 1 = 0$, it follows that $A(1 + A^{2^u-1}) = 0$ for all elements of E.

EXAMPLE 2

Again consider the polynomial $1 + x^{2^6-1} = 1 + x^{63}$

where $q = 6 = 2.3$.

By theorem 3-5-9, we can write:

$$x(1 + x^{63}) = (x + x^8)(1 + (x + x^8)^7) = (x + x^8)(1 + x + x^8)$$
$$(1 + x + x^8 + x^3 + x^{10} + x^{17} + x^{24})$$
$$(1 + x^2 + x^{16} + x^3 + x^{10} + x^{17} + x^{24})$$

also,

$$x(1 + x^{63}) = (x + x^4 + x^{16})(1 + (x + x^4 + x^{16})^3) = (x + x^4 + x^{16})$$
$$(1 + x + x^4 + x^{16})(1 + x + x^4 + x^{16} +$$
$$+ x^2 + x^8 + x^{32})$$

furthermore, by theorem 3-5-8 we have:

$$(x + x^4 + x^{16})(1 + x + x^4 + x^{16}) = (x + x^8)(1 + x + x^8 + x^3 +$$
$$+ x^{10} + x^{17} + x^{24})$$

and also,

$$(1 + x + x^8)(1 + x^2 + x^3 + x^{10} + x^{16} + x^{17} + x^{24}) = 1 + x + x^2 +$$
$$+ x^4 + x^8 + x^{16} + x^{32}.$$

Finally, we note in passing that the preceeding theorems on the factorization of the polynomial $1 + x^{2^q-1}$, find application whenever we require to factor a polynomial of the form $1 + x^m$, where $m = r.n$, and $n = 2^q - 1$, for upon substitution of $y = x^r$, we have

$$1 + x^m = 1 + (x^r)^n = 1 + y^n = 1 + y^{2^q-1}.$$

We now further illustrate, by some examples.

EXAMPLE 3

$$1 + x^{2^4-1} = 1 + x^{15}$$

By corollary 1 to theorem 3-5-3

$$1 + x^{15} = (1 + x + x^2 + x^4 + x^8)(1 + x + x^3 + x^7)$$

By theorem 3-5-8

$$1 + x + x^3 + x^7 = (1 + x^3)(1 + x + x^4)$$

where $q = 4 = 2.2$

the reciprocal of $1 + x + x^4$ must then be a factor of $1 + x + x^2 + x^4 + x^8$ and we find,

$$1 + x + x^2 + x^4 + x^8 = (1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4),$$

therefore,

$$1 + x^{15} = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)$$
$$(1 + x + x^2 + x^3 + x^4).$$

EXAMPLE 4

$$1 + x^{2^5-1} = 1 + x^{31}$$

Because 5 is a prime, it is impossible to make use of theorem 3-5-9. However, by theorem 3-5-3 we have:

$$\begin{matrix} 1 & 2 & 4 & 8 & 16 \end{matrix}$$
$$(1 + x + x^2 + x^4 + x^8 + x^{16})(1 + x + x^3 + x^7 + x^{15}) = 1 + x^{31}$$

$$\begin{matrix} 5 & 10 & 20 & 9 & 18 \end{matrix}$$
$$(1 + x^5 + x^{10} + x^{20} + x^9 + x^{18})(1 + x^5 + x^{15} + x^4 + x^{13}) =$$
$$= (1 + x^4)(1 + x^{31})$$

$$(1 + x^7 + x^{14} + x^{28} + x^{25} + x^{19})(1 + x^7 + x^{21} + x^{18} + x^{12}) =$$
$$= (1 + x^{18} + x^{12})(1 + x^{31})$$

$$(1 + x^{11} + x^{22} + x^{13} + x^{26} + x^{21})(1 + x^{11} + x^2 + x^{15} + x^{10}) =$$
$$= (1 + x^2 + x^{10})(1 + x^{31})$$

$$(1 + x^{15} + x^{30} + x^{29} + x^{27} + x^{25})(1 + x^{15} + x^{14} + x^{13} + x^{10}) =$$
$$= (1 + x^{14} + x^{12} + x^8)(1 + x^{31})$$

$$(1 + x^3 + x^6 + x^{12} + x^{24} + x^{17})(1 + x^3 + x^9 + x^{21} + x^{14}) =$$
$$= (1 + x^{14})(1 + x^{31})$$

making use of the remarks from section 3-2 we find,

$$\text{g.c.d. } (1 + x + x^3 + x^7 + x^{15},\ 1 + x^8 + x^{12} + x^{14} + x^{15}) =$$
$$= 1 + x^2 + x^3 + x^5 + x^7 + x^8 + x^{10}$$

therefore,

$$(x^{10} + x^8 + x^7 + x^3 + x^2 + 1)(x^5 + x^3 + x^2 + x + 1) =$$
$$= x^{15} + x^7 + x^3 + x + 1$$

$$(x^{10} + x^8 + x^7 + x^3 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1) =$$
$$= x^{15} + x^{14} + x^{12} + x^8 + 1$$

also,

$$\text{g.c.d.}\ (1 + x^3 + x^9 + x^{14} + x^{21},\ 1 + x^7 + x^{12} + x^{18} + x^{21}) = \\ = x^{10} + x^6 + x^5 + x^4 + 1$$

$$x^{10} + x^6 + x^5 + x^4 + 1 = (x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^2 + x+1)$$

$$x^{10} + x^8 + x^7 + x^3 + x^2 + 1 = (x^5 + x^3 + 1)(x^5 + x^2 + 1)$$

therefore,

$$1 + x^{31} = (1 + x)(x^5 + x^3 + 1)(x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x + 1) \\ (x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + \\ + x^3 + x^2 + 1).$$

EXAMPLE 5

$$x^{2^9-1} + 1 = x^{511} + 1$$

$$q = 9 = 3.3$$

By theorem 3-5-9, we have:

$$x(1 + x^{511}) = (x + x^8 + x^{64})(1 + (x + x^8 + x^{64})^7)$$

since,

$$1 + y^7 = (1 + y)(1 + y + y^3)(1 + y^2 + y^3)$$

where $y = x + x^8 + x^{64}$

we have,

$$x(1 + x^{511}) = x(1 + x^7 + x^{63})(1 + x + x^8 + x^{64})(1 + (x + x^8 + x^{64}) \\ + (x^3 + x^{17} + x^{129} + x^{10} + x^{24} + x^{136} + x^{66} + x^{80} + \\ + x^{192})(1 + x^2 + x^{16} + x^{128} + x^3 + x^{17} + x^{129} + x^{10} + \\ + x^{24} + x^{136} + x^{66} + x^{80} + x^{192}).$$

Considering the polynomial $1 + x^7 + x^{63} = 1 + x^7 + (x^7)^9$, and letting $z = x^7$, we have $1 + z + z^9 = 1 + z + z^{2^3+1}$ and by theorem 3-4-3 of section 4, it follows that the polynomial $1 + x + x^9$ is irreducible, since no irreducible polynomial of degree 3 will devide $1 + x + x^9$.

EXAMPLE 6

$x^{2^{12}-1} + 1 = x^{4095} + 1$ and $q = 12 = 2.6 = 3.4$.

By theorem 3-5-9 we have:

$$1 - A_1 = x + x^{2^2} + x^{2^{2.2}} + x^{2^{3.2}} + x^{2^{4.2}} + x^{2^{5.2}}$$

where $u = 2$, $v = 6$.

Therefore, $x(1 + x^{2^{12}-1}) = A_1(1 + A_1^3)$ .....(1)

$$2 - A_2 = x + x^{2^3} + x^{2^{2.3}} + x^{3.3}$$

where $u = 3$ $v = 4$

Therefore, $x(1 + x^{2^{12}-1}) = A_2(1 + A_2^7)$ .....(2)

$$3 - A_3 = x + x^{2^4} + x^{2^{2.4}}$$

where $u = 4$ $v = 3$

Therefore, $x(1 + x^{2^{12}-1}) = A_3(1 + A_3^{15})$ .....(3)

$$4 - A_4 = x + x^{2^6}$$

where $u = 6$ $v = 2$

Therefore, $x(1 + x^{2^{12}-1}) = A_4(1 + A_4^{63})$ .....(4)

Furthermore, we know from theorem 5-8-8 that the A_i's must be a factor of $1 + x + x^2 + x^4 + x^8 + x^{16} + x^{32} + x^{64} + x^{128} + + x^{256} + x^{512} + x^{1024} + x^{2048}$.

Furthermore, equations 1, 2, 3, 4 can be further factored since they are all of the form $A_i(1 + A_i^{2^q-1})$. For example, consider the polynomial $1 + x^{15} + x^{255} = 1 + y + y^{17}$ where $y = x^{15}$ of eq. 3. Now by theorem 3-4-3 of section 4, the factors of the polynomial $1 + y + y^{2^4+1}$ have degrees dividing $3.4 = 12$ and periods dividing $2^{12} - 1$. By factoring, we find

$$1 + y + y^{17} = (1 + y + y^2)(1 + y + y^3)(1 + y + y^4 + y^6 + y^8 + + y^9 + y^{10} + y^{11} + y^{12})$$

and it follows that the polynomial $1 + x + x^4 + x^6 + x^8 + x^9 + + x^{10} + x^{11} + x^{12}$,

is irreducible, furthermore upon replacing $y = x^{15}$

$$1 + x^{15} + x^{255} = (1 + x^{15} + x^{30})(1 + x^{15} + x^{45})(1 + x^{15} + x^{60} + + x^{90} + x^{120} + x^{135} + x^{150} + x^{165} + x^{180}).$$

Also, by corrolary 3 to theorem 3-5-3

$$1 + x^{4095} = (1 + x^{65} + x^{130} + x^{260} + x^{520} + x^{1040} + x^{2080})(1 + x^{65} + + x^{195} + x^{455} + x^{975} + x^{2015})$$

where $K = 65 = 2^{12}-1/2^6-1$

different expansions will be gotten by using

$$K = 2^{12}-1/2^4-1 = 273$$

$$K = 2^{12}-1/2^3-1 = 585$$

$$K = 2^{12}-1/2^2-1 = 1365.$$

CONCLUDING REMARKS

It is obvious that the theorems presented in the third chapter do not eliminate the use of certain well known algorithms for direct factorization over a finite field, such as the one recently provided by Berlekamp (13). However, the application of these theorems will simplify the use of these algorithms. The theorems are most helpful when q in the expression $1 + x^{2^q-1}$ is not a prime, and especially if 3 is a factor of q, for it then becomes possible to make use of some known technique for the factorization of trinomials (14) over a GF(2). Finally, further study of polynomials of the form $x^k + x^{2k} + \ldots + x^{2^{(q-1)}k} \pmod{x^{2^q-1} + 1}$, might lead to a method for choosing polynomials of the above form, for which the g.c.d. is easily found.

REFERENCES

1 - R.C. Bose and D.K. Ray - Chaudhuri:
"Further results on error correcting binary group codes",
Information and control, vol. 3, 1960, pp. 279-90.

2 - S.W. Golomb: "Digital Communications".
Prentice Hall, Englewood Cliffs, 1964, p. 11.

3 - R.A. Dean: "Elements of Abstract Algebra".
John Wiley & Sons Inc., 1966, pp. 222-224.

4 - Paley & Weichsel: "A First Course in Abstract Algebra".
Holt - Rinehart - Winston, 1966, p. 89.

5 - Paley & Weichsel: "A First Course in Abstract Algebra".
Holt - Rinehart - Winston, 1966, p. 164.

6 - Peterson: "Error-Correcting Codes".
The M.I.T. Press, Mass. Inst. of Technology,
Cambridge, Mass.

7 - Id. (3), P. 215.

8 - Id. (3), p. 210.

REFERENCES (cont'd)

9 - Bartee and Schneider: "Computations over Finite Fields".
Information and control, vols. 6 - 7, 1963-64, pp. 79-98.

10 - McCarthy: "Algebraic Extension of Fields".
Blaisdell Publishing Co., 1966, p. 24.

11 - Golomb: "Shift Register Sequences".
Holden - Day, Inc., San Francisco, Cal.

12 - Albert: "Fundamental Concepts of Higher Algebra".
The University of Chicago Press, Chicago, 1937, p. 101.

13 - E.R. Berlekamp: "Factoring Polynomials over Finite Fields".
The Bell System Technical Journal, Oct. 1967, pp. 1853-59.

14 - Selmer: "On the Irreducibility of Certain Trinomials".
Math. Scandinavica, Vol. 4, 1956, pp. 287-302.

15 - I.T. Adamson: "Introduction to Field Theory".
Oliver & Boyd, a division of John Wiley & Sons, Inc., 1964, p. 129.

16 - Id. (15), pp. 110-12.

VITAE

Full Name:	Paul Emile Allard
Birth Place:	Pembroke, Ontario
Date:	10 April 1942
High School:	Ecole Superievre de Hull
University:	Ottawa University
Degrees:	B Sc. (Physics) 1964
	B A Sc. (Electrical Engg.) 1966