November 1990 **TR/13/90**

The construction of self-dual normal polynomials over GF(2) and their applications to the Massey-Omura algorithm

by

Dr. Andrew Rae
Mahmood Khan Pathan

THE CONSTRUCTION OF SELF-DUAL NORMAL POLYNOMIALS

OVER GF(2) AND THEIR APPLICATIONS TO

THE MASSEY-OMURA ALGORITHM

Dr. Andrew Rae
Mahmood Khan Pathan

Abstract

Gaussian periods are used to locate a normal element of the finite field $GF(2^e)$ of odd degree e and an algorithm is presented for the construction of self-dual normal polynomials over GF(2) for any odd degree. This gives a new constructive proof of the existence of a self-dual basis for odd degree. The use of such polynomials in the Massey-Omura multiplier improves the efficiency and decreases the complexity of the multiplier.

This work is part of the Ph.. D thesis of M. K. Pathan (in preparation under the supervision of Dr. A. Rae).

Introduction

Finite field arithmetic is necessary for the construction of some well known error-correcting codes [5] and normal bases of finite fields are important for the implementation of computational algorithms in $GF(2^m)$, see [6], [8] and [12] - [15]. The existence of at least one normal basis for every finite extension of GF(2) is well known [2], but to locate a normal basis of a finite field is a problem [11].

In this report an algorithm is presented for the construction of self-dual normal polynomials over $GF(2)$; we conjecture that, in addition, these polynomials are always primitive. This algorithm uses the Gaussian periods of cyclotomy theory to locate a normal element and its conjugates in an extension of the Galois field, GF(2). The polynomials constructed from Gaussian periods are irreducible over GF(p), see [1]. These polynomials are applied to the Massey-Omura algorithm [15] and it is found that they make the Massey-Omura multiplier faster by reducing its complexity. The structure of the multiplier under the application of these polynomials requires less silicon chip area than that required in algorithm proposed by Wang in [11].

Section 1 discusses the Massey-Omura algorithm and explains the structure of Massey-Omura Multiplier for $GF(2^m)$ together with the relevant related terms.

Section 2 defines the necessary terms and notations and presents an algorithm for the construction of self-dual normal polynomials over GF(2). The method for the calculation of the Massey-Omura Number of a binary normal polynomial is also described.

Section 3 presents an application of the algorithm described in section 2 and constructs a list of self-dual normal polynomials of odd degree ≤ 99 over $GF(2)$ together with the

Massey-Omura Numbers associated with them.

section 4 generates all polynomials of trace 1 and odd degree ≤ 13 over $GF(2)$ and calculates the Massey-Omura number for each of them. A table is produced which illustrates the lower and upper bounds of the Massey-Omura multiplier for $GF(2^m)$, where m is odd and ≤ 13.

Section 1

1.1 Massey-Omura algorithm

Finite fields are used in most of the known constructions of codes, and *GF* (2^m), the finite extension of *GF* (2) of degree m, is of particular interest because computations for Reed-Solomn codes and Bose-Choudhri-Hocquenghem codes (BCH-codes) take place in this field. The use of GF(2^m) in secret communications has made it very important, *GF* (2^m) is the only class of finite fields considered in this report.

The operation of multiplication in GF(2^m) is complex and, therefore, more time consuming than ordinary binary multiplication. Addition, on the other hand, is easy and straight forward. Recently, a pipeline architecture based on the Massey-Omura algorithm was developed to compute multiplication in *GF* (2^m), see [15]. The Massey-Omura algorithm utilizes a normal basis,

$$\beta = \{\alpha, \alpha^2, \alpha^4, \ldots\ldots, \alpha^{2m-1}\}$$

to represent the elements of the field *GF*(2^m), where α is a root of an irreducible polynomial of degree *m* over *GF* (2).

In the normal basis representation, squaring of an element of the field is a simple cyclic shift of its binary digits and multiplication requires the same logic circuitry for any product digit as it does for any other product digit. Adjacent product digit circuits differ only in their inputs, which are cyclically shifted versions of one another.

1.2 Massey-Omura multiplier

The work originally described by Massey and Omura is reviewed in [15] as follows:-

It is known that there always exists a normal basis in *GF*(2^m) for all positive integers *m,* see [2], so that one can find an element a such that $B = \{ \alpha, \alpha^2, \ldots\ldots, \alpha^{2^{m-1}} \}$ is a basis for $GF(2^m)$. Thus every element β of the field $GF(2^m)$ can be expressed uniquely as

$$\beta = \sum^{m-1} b_i \alpha^{2^i} \quad \text{where } b_i \in GF(2).$$

Suppose that the set B is a normal basis for $GF(2^m)$, then by utilizing the properties of Galois fields,

$$\beta^2 = b_{m-1}\alpha + b_0\alpha^2 + b_1\alpha^4 + b_{m-2}\alpha^{2m-1}.$$

Thus, if β is represented in vector form, i.e.,

$$\beta = [b_0, b_1, b_2, \ldots, b_{m-1}] \text{ then } \beta^2 = [b_{m-1}, b_0, b_1, \ldots, b_{m-2}].$$

Hence, in the normal basis representation β^2 is a cyclic shift of β.

Let $\beta = [b_0, b_1, b_2, \ldots, b_{m-1}]$ and $\gamma = [c_0, c_1, c_2, \ldots\ldots\ldots, c_{m-1}]$ be two arbitrary elements of $GF(2^m)$ expressed in the normal basis. Then the last term d_{m-1} of the product $\delta = \beta\gamma = [d_0, d_1, d_2, \ldots, d_{m-1}]$ is some binary function of the components of β and γ. i.e.,

$$d_{m-1} = f(b_0, b_1, b_2, \ldots, b_{m-1}; c_0, c_1, c_2, \ldots, c_{m-1}). \quad (1)$$

Since squaring means a cyclic shift of the components of the element expressed in normal basis, one has $\delta^2 = \beta^2 \gamma^2$, or equivalently,

$$[d_{m-1}, d_0, d_1, \ldots d_{m-2}] = [b_{m-1}, b_0, b_1, \ldots b_{m-2}] \,.\, [c_{m-1}, c_0, c_1, \ldots c_{m-2}].$$

Hence, the last component, d_{m-2} of δ^2, is obtained by the same function f in (1), i.e.,

$$d_{m-2} = f(b_{m-1}, b_0, b_1, \ldots, b_{m-2}; c_{m-1}, c_0, c_1, \ldots, c_{m-2}).$$

By squaring δ repeatly, the rest of the product digits can be found by the same binary function f, and we get

$$\left.\begin{aligned} d_{m-1} &= f(b_0, b_1, b_2, \ldots\ldots, b_{m-1} ; c_0, c_1, c_2, \ldots\ldots, c_{m-1}) \\ d_{m-2} &= f(b_{m-1}, b_0, b_1, \ldots\ldots, b_{m-2} ; c_{m-1}, c_0, c_1, \ldots\ldots, c_{m-2}) \\ &\vdots \\ d_o &= f(b_1, b_2, \ldots\ldots, b_{m-1}, b_0 ; c_1, c_2, \ldots\ldots, c_{m-1}, c_0) \end{aligned}\right\} \quad ..(2)$$

The expressions in (2) define the Massey-Omura multiplier for $GF(2^m)$.

1.3 Massey-Omura Number (MON)

The number of terms in the binary function f of (1) is called the Massey-Omura number and we denote it by MON.

1.4 Normal basis in GF(2^m)

It is known that for m $\geq$ 4 there is more than one irreducible polynomial which generates $GF(2^m)$ and such that the set of its roots is linearly independent and so a normal basis. Therefore a Massey-Omura multiplier (MOM) for $GF(2^m)$ has more than one structure for $m \geq 4$. The complexity of the implementation of the Massey- Omura algorithm depends on the Massey-Omura number (MON). Now the MON depends on the generating polynomial of the field $GF(2^m)$, it is clearly desirable to find a polynomial which produces the least possible MON for the multiplier.

Wah and Wang used irreducible "all-one-polynomials", (which they call AOPS),

$$p(x) = \sum_{i=0}^{m} x^i ,$$

to generate the elements of the field $GF(2^m)$. Such polynomials yield ($2m$-1) as MON, see [10]. In that paper they prove the following theorem.

"If and only if (m + 1) is prime and 2 is a primitive root modulo (m + 1) then AOP of degree m is irreducible and its roots α^{2^i}, , i = 0,1,2,……, m - 1, form a normal basis for GF(2^m)."

Wang in [12] demonstrated that if p is a prime and 2 is a primitive root modulo p^n where n is a positive integer and $m = 2^k p^n$ for $k \geq 0$ then following conditions are sufficient to locate a normal basis for $GF(2^m)$.

$Let\ \alpha \in GF(2^m)$ and

(i) $\mathrm{Tr}(\alpha) = 1$

(ii) $g_j^{(m)}(\alpha) \neq 0$, for $j = 1,2,.....,n$ where

$$g_j^{(m)}(\alpha) \neq 1 + \sum^{(\frac{m}{p})-1} \alpha^{2ip} \quad \text{and}$$

$$g_j^{(m)}(\alpha) = 1 + \sum_{\substack{i=0 \\ p \times i}}^{(\frac{m}{p^{i-1}})-1} \alpha^{2ip^{j-1}} \quad \text{for} \quad (2 \leq j \leq n)$$

then $\{\alpha, \alpha^2, \ldots, \alpha^{2m-1}\}$ is a normal basis for $GF(2^m)$.

But the selection of an element α which fulfills the above mentioned conditions, is itself a problem. Wang in [11] adopted the trial and error method to find such an element. He also developed a method for the location of self-dual normal basis for $GF(2^m)$ of odd degree m.

By calculating the MON for the two type of basis mentioned above for various degrees, he observes that self-dual normal polynomials generate a low MON compared to normal polynomials of the same degree, see [11].

Section 2

In this section an algorithm for the construction of binary normal polynomials is presented. This algorithm uses the Gaussian periods of cyclotomy theory to locate a normal element and its conjugates in the Galois field, $GF(2^e)$ and so to construct a normal polynomial of degree *e*. (Aldeman and Lenstra proved in [1] that polynomials constructed from Gaussian periods are irreducible over GF(p)). This algorithm can also, with the introduction of an extra condition, be used to construct binary self-dual normal polynomials.

2.1 Terms and notations

2.1.1 Normal polynomials over GF(2)

An irreducible polynomial, $p(x)$ of degree m over $GF(2)$ is a normal polynomial if the set of its roots is linearly independent over $GF(2)$. In other words, the set of roots of $p(x)$ is a basis for the vector space $GF(2^m)$.

2.1.2 Trace of an element of $GF(2^m)$

The trace of an element α of $GF(2^m)$ over $GF(2)$ is the sum of the conjugates of α with respect to $GF(2)$ and denoted by Tr(α).

2.1.3 Self-dual normal bases for $GF(2^m)$

The normal polynomial $p(x)$ is self-dual if the set of its roots constitutes a self-dual basis for $GF(2^m)$. A basis B = { $\gamma_1, \gamma_2, \ldots \gamma_n$ } is self-dual if

$$Tr(\gamma_i \gamma_j) = \delta_{ij} \qquad where \;\; \delta_{ij} = \begin{cases} 1 & if \;\; i=j \\ 0 & if \;\; i \neq j \end{cases}$$

2.1.4 Order of 2 mod *p*

Let p be a prime, a positive integer m is the order of 2 *mod p if* $2^m \equiv 1 \mod p$ and $2^d \neq 1 \mod p$ *for d /m* and $d < m$.

2.1.5 Primitive root mod p

A positive integer g is a primitive root of a prime p if $g^{p-1} \equiv 1\ 1 \mod p$ and

$g^i \neq l \mod p$, for i=1,2, ….,p-2.

2.2 The construction of self-dual normal polynomials

2.2.1 Theorem

Let $p = ef + 1$ be a prime for some positive integers e and f. Suppose the order of 2 mod p is m and

$$d = \frac{(p-1)}{m}.$$

If g is a primitive root mod p, then let

$$\eta_j = \sum_{i=0}^{f-1} \zeta^{g^{ei+j}} \qquad \text{for } j = 0,1, \ldots, e\text{-}1$$

where $\zeta = exp\frac{2\pi i}{p}$ is a primitive p th root of unity and

$$\tilde{q}(x) = \prod^{e-1}(x - \eta_j) \in Z[X].$$

Let $q\ (x)$ be the polynomial over Z_2 obtained by taking the coefficients of

$\tilde{q}$ (x)modulo 2 then

q (x) is irreducible and normal over GF (2) if and only if $(e, d) = 1$.

Moreover, it is self-dual if and only if f is even.

Note: We conjecture that in addition p (x) is always primitive if p is the least prime satisfying, for a given e, $p = ef + 1$ for some f and $(e, d) = 1$.

Proof:-

For the proof of irreducibility of $p(x)$ see [1] and for normality and self-duality see [3].

2.2.2 Definition

The η_j for $j = 0, 1, \ldots\ldots, e-1$ of theorem 2.2.1 are called the **Gaussian e-periods of f-terms** or simply **Gaussian periods.** And any period of f-terms can be determined rationally from another period of f-terms [9, page 243].

we shall call the irreducible binary normal polynomial constructed from a Gaussian period, a **Gaussian polynomial** and denote it by **GP(x).**

2.2.3 Corollary:

Every Gaussian polynomial of odd degree is self-dual.

Proof :-

Let GP(x) be a Gaussian polynomial of odd degree e.

Since, GP(x) is a Gaussian there is an integer f with $ef + 1$ a prime p.

Now, $f = (p-1)/e$ is an even integer.

Hence, theorem (2.2.1) implies that GP(x) is self-dual.

Gaussian polynomials of even degree are studied in [3], we have also developed another algorithm to construct the Gaussian polynomials of 2-term over GF (2) which enables us to construct such polynomials of degrees up to 2,993.

2.3 Self-duality test for Gaussian polynomials

Let α be a root of Gaussian Polynomial, GP(x) of degree n, and

$B = \{\alpha^{2^i} \mid i = 0, 1, \ldots, n-1\}$ be a normal basis of the field K = GF (2^n).

If $\mathrm{Tr}\ (\alpha\, \alpha^{2^i}) = \mathrm{Tr}\ (\alpha^{2^i+1}) = 0$, for $i = 1, 2, \ldots\ldots, n-1$

then B is a self-dual basis for K. But, if n is odd then

$$\mathrm{Tr}(\alpha^{2^i+1}) = Tr\,(\alpha^{2^{n-i}+1}).$$

Thus if

$$\mathrm{Tr}(\alpha^{2^i+1}) = 0 \text{ for } i = 1, 2, \ldots, (n-1)/2$$

then B *is* a self-dual normal basis *of* K and hence GP(x) is a self-dual polynomial.

2.4 Calculation of the Massey-Omura number of a Gaussian polynomial

Suppose $B = \{\alpha_i = \alpha^{2i} \mid i = 0,\ldots,n\text{-}l\}$ is a normal basis for $GF(2^n)$.

Let $\alpha = \alpha_0$ and suppose

$$\alpha_i \cdot \alpha_j = \sum_{k=0}^{n-1} aijk \cdot \alpha_k \text{ where } a_{ijk} \in Z_2 \text{ for each } i\, j$$

then the product function $f : Z_n \times Z_n \rightarrow Z_2$ is defined by $f(i, j) = a_{ij0}$

and the MON = $\sum_{i,j=0}^{n-1} aijo$ where the sum is taken in Z.

2.4.1 Definition

If V is a vector space of finite dimension over GF (2) and B is a basis then w (λ), the weight of λ ε K is the number of non-zero coordinates of λ, with respect to *B*.

2.4.2 Theorem

Let $K = GF(2^n)$ and $p(x)$ be an irreducible normal polynomial of degree n over $GF(2)$.
If $w(\lambda.)$ is the weight of $\lambda \in K$ with respect to the normal basis,

$$\{\alpha^{2i} \mid i = 0, 1, 2, \ldots, n\text{-}1\}$$

consisting of the roots of $p(x)$, of K then the Massey-Omura number associated with $p(x)$ is given by the following formula;

$$\text{MON} = \sum_{i=0}^{n-1} w(\alpha^{2i+1}).$$

Further, if we let $w_i = w(\alpha^{2i+1})$ then

$$\text{MON} = 1 + \sum_{i=0}^{\frac{n-1}{2}} w_i \qquad \text{for odd n and}$$

$$\text{MON} = 1 + w_{\frac{n}{2}} + \sum_{i=0}^{\frac{n-1}{2}} w_i \quad \text{for even n.}$$

Proof

Suppose { β_i | i =0,l,...,n -1 } is the dual basis to {α_i}, (For any basis B of K there exist a basis dual to ***B**,* see [2])

then $f(i,j) = \mathrm{Tr}(\alpha_i\,\alpha_i\,\beta_0)$ since $a_{ijk} = \mathrm{Tr}(\alpha_i\,\alpha_i\,\beta_k)$.

Therefore, putting $\beta_o=\beta$

$$\text{MON} = \sum_{i\,j=0}^{n-1} Tr(\sigma^i(\alpha)\sigma^j(\alpha)\beta) \text{ where } \sigma : \lambda \to \lambda^2$$

Now let G be the automorphism group of GF (2^n) over $GF(2)$. G has order n and is cyclic, generated by the Frobenius automorphism σ, see [2].

Thus,

$$\text{MON}= \sum_{\rho\,\in\,G}\sum_{\tau\,\in\,G} Tr\,[\,\rho(\alpha)\,\tau(\alpha)\beta\,]$$

$$= \sum_{\rho}\sum_{\tau} Tr\rho(\alpha\,\tau\rho^{-1}(\alpha)\ \rho-^{1}(\beta)) \quad \text{since } \tau\rho^{-1} = \rho^{-1}\tau \text{ as G is cyclic.}$$

$$= \sum_{\rho}\sum_{\tau} Tr(\alpha\,\tau\rho^{-1}(\alpha)\,\rho^{-1}\beta) \text{ since } Tr(\rho\lambda) = Tr(\lambda)$$

$$= \sum_{\rho}\sum_{\tau} Tr\ (\alpha\ \tau\ (\alpha)\,\rho(\beta))$$

since for a fixed ρ , $\tau\rho^{-1}$ runs through the elements of G as τ does and ρ runs through the elements of G as ρ^{-1} does.

$$= \sum_{\tau\,\in\,G}\ \sum_{j=0}^{n-1}\ Tr\ (\alpha\ \ \tau(\alpha)\beta_j)$$

$$= \sum_{\tau\,\in\,G} w\ (\alpha\,\tau(\alpha\alpha) \text{ where w } (\lambda) \text{ is the weight of with respect to } B.$$

$$= \sum_{i=0}^{n-1} w\ (\alpha_i\ \ \alpha)$$

$$= \sum_{i=0}^{n-1} w(\alpha^{1+2i}) = w_i$$

Now, if $i = 0$, $\alpha^{1+2i} = \alpha^2 = \alpha_2$ and $w(\alpha_2) = 1$.

Also, $(\alpha^{1+2i})^{2n-i} = \alpha^{2n-i+1}$, since α has order dividing $2^n - 1$, the order of the multiplicative group of non-zero elements of $GF(2^n)$. It follows that

$$w_i = w_{n-i}.$$

Hence, the Massey-Omura Number can be calculated by the following formulae:-

$$MON = 1 + 2\sum_{i=0}^{\frac{n-1}{2}} w_i \qquad \text{for odd n,}$$

$$MON = 1 + w_{\frac{n}{2}} + 2\sum_{i=0}^{\frac{n-1}{2}} w_i \qquad \text{for even n.}$$

2.4.3 Corollary

If α is primitive then MON $\geq 2n - 1$.

Proof

In this case, $w_i \geq 2$ for all $i \neq 0$, since

$$\alpha^{2i+1} = \alpha^{2i}$$

is impossible. Thus,

if n is odd then
$$MON \geq 1 + 2\cdot\frac{n-1}{2}\cdot 2$$
$$\geq 1 + 2 + 2n - 4 = 2n - 1,$$

and if n is even then
$$MON \geq 1 + 2 + 2\cdot\frac{n-2}{2}\cdot 2$$
$$\geq 1 + 2 + 2n - 4 = 2n - 1.$$

Note that the AOPs give us MON equal to $(2n - 1)$, and α in this case is not primitive since it has order $(n + 1)$, see [10]. It seems likely that in all cases MON $\geq 2n - 1$.

Section 3

In this section we construct Gaussian polynomials, GP(x) of odd degree ≤ 99, according to the method described in section 2.2. A data-table (3.1) is given for the construction of those GP(x)' ε which fulfill the conditions stated in theorem 2.2.1. Using table (3.1) we have produced a list of GP(x)'s of odd degree ≤ 99 with their Massey-Omura Numbers (MON). The MON of each GP(x) is calculated by the method described in section 2.4, but in all these cases the MON is in fact given by the following formula:

$$\mathrm{MON} = p-(f-2)^2-f \qquad (*)$$

where p is the least prime for a given degree, e, which satisfies the conditions of theorem 2.2.1 and f is even and equal to $(p-1)/e$.

We conjecture that this formula holds for all such (e, p).

Note that formula (*) does not require knowledge of the GP(x), so the MON of a Gaussian polynomial, can be calculated directly from the data-table (3.1) without even constructing the polynomial.

The Gaussian polynomials with $f = 1$ are all-one-polynomials over GF(2) because $e = P-1$ when $f = 1$, and if (e, p) fulfills the conditions of theorem 2.2.1 the GP(x) will be the cyclotomic polynomial of degree $e = p-1$, i.e.,

$$\frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i, \qquad [9, \text{page } 121].$$

The Massey-Omura number associated with an all-one-polynomial of degree e is equal to $2e$-1, see [10].

There is an irreducible AOP of degree n for the following positive integers n < 2000.

2, 4, 10, 12, 18, 28, 36, 52, 60, 66, 82, 100, 106, 130, 138,148, 162, 172,178, 180, 196, 210, 226, 268, 292, 316, 346, 348, 372, 378, 388, 418,420, 442, 460, 466, 490, 508, 522, 540, 546, 556, 562,586, 612, 618, 652, 658, 660, 676,700, 708, 756, 772, 786, 790, 820, 826, 828, 852, 858, 876, 882, 906, 940, 946, 1018, 1060, 1090, 1108, 1116, 1122, 1170, 1186, 1212, 1228, 1236, 1258, 1276, 1282, 1291, 1300, 1306, 1372, 1380, 1426, 1450, 1452, 1482, 1492, 1498, 1522, 1530, 1548, 1570, 1618, 1620, 1636, 1666, 1668, 1692, 1732, 1740, 1746, 1786, 1860, 1866, 1876, 1900, 1906, 1930, 1948, 1972, 1978, 1986, 1996.

The construction of Gaussian polynomials

Let p, m, d and g be as in theorem 2.2.1; values of these are given in data-table (3.1). Rather than working in the complex numbers it is simpler just to let ζ satisfy

$$\sum_{i=0}^{p-1} \zeta^i = 0$$

as remarked by Aldeman and Lenstra in [1]. Then $\zeta^p = 1$, and if

$$\alpha = \sum_{i=0}^{f-1} \zeta^{g^{ei}} \qquad \text{where } p=ef+1 \text{ then}$$

$$P(x) = \prod_{i=0}^{e-1} (x - a^{2i})$$

is the polynomial mentioned in theorem 2.2.1.

Since $(d, e) = 1$, $p(x)$ is irreducible and normal over $GF\,2$, see [3].

We conjecture that if p is least for a Gaussian polynomial, GP(x) of degree e with $f \geq 2$ then GP(x) is best possible in the class of self-dual primitive polynomials for the Massey-Omura multiplier.

Table (3.1)

Data for the construction of Gaussian polynomials.

e	f	p	m	d	g
3	2	7	3	2	3
5	2	11	10	1	2
7	4	29	28	1	2
9	2	19	18	1	2
11	2	23	11	2	5
13	4	53	52	2	5
15	4	61	60	1	2
17	6	103	51	2	5
19	10	191	95	2	19
21	10	211	210	1	2
23	2	47	23	2	5
25	4	101	100	1	2
27	6	163	162	1	2
29	2	59	58	1	2
31	10	311	155	2	17
33	2	67	66	1	2
35	2	71	35	2	7
37	4	149	148	1	2
39	2	79	39	2	3
41	2	83	82	1	2
43	4	173	172	1	2
45	4	181	180	1	2
47	6	283	94	3	3
49	4	197	196	1	2
51	2	103	51	2	5
53	2	107	106	1	2
55	12	661	660	1	2
57	10	571	114	5	3
59	12	709	708	1	2
61	6	367	183	2	6
63	6	367	183	2	6
65	2	131	130	1	2
67	4	269	268	1	2
69	2	139	138	1	2
71	8	569	284	2	3
73	4	293	292	1	2
75	10	751	375	2	3
77	6	463	231	2	3
79	4	317	316	1	2
81	2	163	162	1	2
83	2	167	83	2	5
85	12	1021	340	3	10

e	f	p	m	d	g
87	4	349	348	1	2
89	2	179	178	1	2
91	6	574	546	1	2
93	4	373	372	1	2
95	2	191	95	2	2
97	4	389	388	1	2
99	2	199	99	2	3

Notations

e = Degree of GP(x)
f = terms of Gaussian period
p = ef + 1, a prime
m = Order of 2 mod p
d = (p-1)/m
g = primitive root mod p

Table(3.2)
2 Gaussian polynomials over GF(2)

Degree of GP (x)	Octal rep. of binary coef. of GP (x)	MON
3	15	5
5	67	9
7	323	21
9	1563	17
11	6435	21
13	32231	45
15	151241	53
17	677253	81
19	3204523	117
21	15651031	137
23	64200721	45
25	322317037	93
27	1511057007	141
29	6701600007	57
31	32030414221	237
33	156300600003	65
35	643503200015	69
37	3223713043611	141
39	15040164200321	77
41	67140034601563	81
43	322537325055651	165
45	1511745421752247	173
47	6451364772333755	261
49	32237351036237623	189
51	150720640000016415	101
53	670163340000003467	105
55	3211613547057550725	549
57	15656560421637245317	497
59	64363256503477237461	597
61	337331141424155523331	345
63	1512275147532361651157	357
65	6714030000140000000003	129
67	32253410677275255020135	261
69	156034670003340000000067	137
71	644761733324114426651055	525
73	3223707334516321272752267	285
75	15041742436064444052315553	677
77	67666232077616666304325207	441
79	322535414214733764746701461	309
81	1563006000003460140000671403	161

Table(3.2)(Cont:)
Gaussian Polynomials over GF(2)

Degree of GP(x)	Octal rep.of binary coef.of GP(x)	MON
83	6435032000000720640003216415	165
85	32116501100530277432104602605	909
87	1512566053516263166737454475347	341
89	6714003460000000007140334600163	177
91	3222136133112453101051001155015	525
93	15117457664156203226071724731705	365
95	642004000020000000000072100200001	189
97	322370664246422512173021335737063	381
99	15072064000320000000000003503200015	197

Notations

MON stands for the Massey-Omura Number of GP(x). The octal representation of the binary coefficient vector of GP(x) is explained in the following example.

Example:

Octal form **1563** represents 1101110011, i.e.,

$$x^9 + x^8 + x^6 + x^5 + x^4 + x + 1$$

The Gaussian polynomials constructed under theorem 1 generate less MON than the self-dual normal polynomials produced by Wang [11]. The following table(3.3) illustrates the difference between the MON resulting from the two methods

Table (3.3)

Comparison of Massey-Omura Number			
Degree of the field	MON produced by		
	Gaussian poly	Wang's method	
		normal	Selfdual
7	21	27	-
9	17	-	29
17	81	137	117
30	59	443	-
31	237	-	453
127	501	8123	8049

Section 4

Construction of all irreducible polynomials of trace one and degree ≤ 13

Let p(x) be an irreducible polynomial of degree m and order $q = 2^m - 1$ over *GF(*2), a list of such primitive polynomials, one of each degree $\leq$ 100 is given in [2].

Let $K = GF(2)[x]/(\mathrm{p}(x))$. Then k has order 2^{m}.

Let $K^* = K - \{ 0 \}$. Then (K^*,.) is a cyclic group generated by a root α of p(x) and

$$\rho : K^* \rightarrow Z_q \text{ denned by } \rho(\alpha^i) = i$$

is an isomorphism between (K^*,.) and $(z_q, +)$.

Let i be a member of Z_q. Then if

$$2^{d} \cdot i \neq i \bmod (q) \quad \text{for } d \mathrm{I} m \text{ and } d < m,$$

we say that the set $S = \{i, 2i, 4i, \ldots\ldots, 2^{m-1}i\}$ is the orbit of i under multiplication by 2 and that it has length *m.*

Now, we claim that α^i is a generator of K over *GF* (2) if $i \neq 0$.

Thus $pi\,(x) = \prod_{j=0}^{m-1}\left(x - \left(\alpha^{i}2^{i}\right)\right)$ is an irreducible polynomial of degree *m,* and if

$$\sum_{i=0}^{m-1}\left(\alpha^{i2i}\right) = 1$$

then it has trace 1.

Conversely, if α^i generates K over GF (2) its m conjugates will be

$\{\alpha^{i2j} 1 j = 0, 1, \ldots, m-1\}$ so that the orbit of i has length *m.*

Thus we obtain all irreducible polynomials of degree *m* by taking all orbits of length *m* inZ_q.

The normality and self-duality of i $p_i(x)$ s determined as explained in sec. 2.1.1 and 2.1.3 respectively and the Massey-Omura number of the normal polynomials is calculated according to the method described in section 2.4.

A table (appendix A) of polynomials of odd degree $\leq$ 13 and trace 1 is produced with their orders and respective Massey-Omura numbers. The polynomials in the appendix A are represented in octal form. The suffix N of the octal representation indicates a normal polynomial and suffix NS shows that polynomial is normal and self-dual.

Table (4.1) consists of the lower and upper bounds for the Massey-Omura Number of the finite field of odd degree $\leq$ 13 taken from appendix A.

The comparison of lower bound with the MON generated by Gaussian polynomials of odd degree $\leq$ 13, shows that Gaussian polynomials achieve these bounds except for degree 7.

Table (4.1)

	Massey-Omura Number	
Degree	Lower bound	Upper bound
3	5	5
5	9	15
7	19	27
9	17	45
11	21	71
13	45	101

Conclusion

An algorithm for the construction of normal and self-dual normal polynomials over GF(2) is presented and a table (3.2) of these is given for odd degrees up to 99.

The study of table (3.2) reveals that the proposed algorithm improves the efficiency of the Massey-Omura Multipliers for $GF(2^m)$ by reducing their complexity.

The table (3.3) of comparisons of this algorithm with the method proposed by Wang in [8] illustrates that Gaussian polynomials generates much lower Massey-Omura numbers than those polynomials produced by Wang's methods.

It is also evident from table (4.1) that the Gaussian polynomials of odd degree $\leq$ 13 achieve the least possible bounds except for that of degree 7.

Refrences

[1] Adleman, L.M and Lenstra Jr., H.W., *Finding irreducible polynomials over finite Fields* Proc. 18th Annual ACM SYMP on Theory of computing (STOS). 1986, pp. 350-355.

[2] Lidl, Rudolf and Harald Niederreiter, *Finite Fields,* Cambridge University Press, 1987.

[3] Pathan, Mahmood K., *Ph.D thesis in preparation.*

[4] Pei, Din Y., Charls C. Wang and Jim K. Omura, *Normal Basis of finite field GF(2^m)*, IEEE Trans. Inf. Th., Vol. IT-32, No. 2, March 1986.

[5] Peterson, W. W. and Weldon Jr., E. J., *Error-Correcting Codes,* MIT Press, Cam bridge, 1972.

[6] Pincin, A., *A New Algorithm for Multiplication in Finite Fields,* IEEE Trans. Comp., Vol. 38, No.7, July 1989.

[7] Rivlin, Theodore J., *The Chebyshev Polynomials,* John Wiley & Sons, 1974.

[8] Shayan, Y. R., and T. Le-Ngoc, *The least complex parallel Massey-Omura multi - plier and its LCA and VLSI designs,* IEEE Proceedings, Vol. 136, Pt. G, No. 6, December 1989.

[9] Tignol, Jean-Pierre, *Galois' theory of algebraic equations,* Longman scientific & technical, 1987.

[10] Wah, P. K. S. and M. Z. Wang, *Realization and application of the Massey-Omura lock,* Digital Comm., Int. Zurich Seminar, IEEE Press, 1984, pp. 175 - 182.

[11] Wang, C. C., *Exponentiation in Finite Field GF(2^m),* Ph.D dissertation, School of Engineering and applied Sciences, UCLA, Feb. 1985.

[12] Wang, C.C., *A generalized algorithm to design finite field normal basis multipliers,* TDA Progress Report 42 - 87, July - Sept. 1986, PP. 125 -139.

[13] Wang, Charles C., *An algorithm to design finite field multipliers using a self-dual normal basis,* IEEE Trans. Comp., Vol. 38, No. 10, Oct. 1989, PP. 1457 – 1460.

[14] Wang, Charles C. and Pei, Dingyi, *A VLSI design for computing exponentiations in GF(2^m)* and their application to generate Pseudorandom number sequence, IEEE Trans. Comp., Vol. 39, No. 2, Feb. 1990, PP. 258 - 262.

[15] Wang, Charles C, T.K. Truong, H.M. Shao, J.L. Deutsch, Jim K. Omura and Irving S. Reed, *VLSI architectures for computing multiplications and inverses in GF(2^m)*, IEEE Trans. Comp. Vol. C - 34, No. 8, August 1985, PP 709 - 716.

APPENDIX (A)

Polynomials of trace 1		
Order	P(x)	MON
Degree = 3		
7	15NS	5
Degree = 5		
31	67NS	9
31	75N	15
31	73N	11
Degree = 7		
127	323NS	21
127	345N	19
127	313N	21
127	301N	21
127	325N	25
127	357N	27
127	367N	27
127	361	--
127	375	--
Degree = 9		
511	1563NS	17
511	1517NS	29
73	1511NS	29
511	1461N	41
511	1743N	35
73	1401N	41
511	1423N	41
511	1773N	35
511	1671N	43
511	1553N	45
511	1617N	39
511	1731N	31
511	1473N	37
511	1605N	39
511	1707N	39
511	1725N	39
511	1555N	29
511	1533N	29
511	1713N	31
511	1425N	41
511	1437N	37
511	1665	--
511	1541	--

Polynomials of trace 1		
Order	P(x)	Order
511	1715	--
511	1443	--
511	1577	--
73	1641	--
511	1751	--
Degree = 9		
2047	6435NS	21
2047	6741NS	57
2047	6447NS	45
89	7773N	51
2047	7565N	63
2047	7633N	55
2047	7063N	55
2047	6543N	61
2047	7745N	59
2047	7137N	67
2047	7053N	51
2047	6403N	65
2047	6637N	53
89	73 1N	43
2047	6673N	45
2047	7535N	43
2047	6211 N	57
2047	665I N	53
2047	7335N	55
2047	7071N	55
2047	6235N	61
2047	6227N	49
2047	6623N	53
2047	7107N	59
89	606 N	49
2047	7173N	63
2047	7047N	63
2047	7371N	47
2047	7125N	55
2047	7041N	55
2047	7035N	63
2047	7655N	59
2047	7603N	55
2047	6013N	49
2047	6417N	57

Polynomials of trace 1		
Order	P(x)	MON
2047	6263N	57
2047	6747N	49
2047	7273N	63
2047	6557N	65
2047	7627N	59
2047	6037N	49
2047	6325N	49
2047	7467N	51
2047	6675N	57
2047	6163N	53
2047	6015N	61
2047	7175N	59
2047	6501N	65
2047	7461N	47
2047	6507N	53
2047	7317N	59
2047	7237N	71
2047	6323N	61
2047	6315N	69
2047	6733N	61
2047	7647N	59
89	6777N	61
89	7571N	55
2047	7363N	55
2047	6205N	53
2047	6277N	53
2047	7621N	47
2047	7715N	55
2047	7113N	55
2047	6233N	65
2047	6127N	53
2047	6711N	49
2047	7553N	43
2047	6367N	61
2047	7223N	55
2047	6343N	53
2047	6141N	65
2047	7201N	59
2047	7723N	59
2047	6727N	61
2047	7243N	67
23	6165N	41
2047	7161N	59
2047	7413N	63
2047	6455N	53

Polynomials of trace 1		
Order	P(x)	MON
2047	7555N	63
2047	6561N	61
2047	6153N	49
2047	7751N	71
2047	7005N	51
2047	6765N	61
2047	6351N	49
2047	6531N	49
2047	6307N	49
2047	7431N	67
2047	7665N	51
2047	6031N	65
2047	6525N	57
Degree =13		
8191	32231NS	45
8191	33417NS	57
8191	32101NS	69
8191	33735NS	57
8191	33523NS	81
8191	35345N	91
8191	37775N	87
8191	37611N	83
8191	33343N	77
8191	34035N	71
8191	35337N	91
8191	33357N	73
8191	36441N	83
8191	34605N	87
8191	36043N	79
8191	30667N	77
8191	36253N	67
8191	36271N	71
8191	37527N	75
8191	37005N	87
8191	34341N	79
8191	33741N	81
8191	35531N	87
8191	36117N	71
8191	34311N	87
8191	30711N	57
8191	31521N	85
8191	33471N	73
8191	34401N	75
8191	37151N	75
8191	34715N	91

Polynomials of trace 1		
Order	p(x)	MON
8191	30537N	61
8191	31327N	97
8191	32461N	77
8191	35277N	83
8191	35667N	83
8191	30221N	81
8191	33643N	77
8191	30241N	69
8191	33111N	77
8191	31231N	77
8191	37665N	83
8191	33455N	85
8191	31633N	97
8191	37275N	87
8191	37145N	71
8191	33013N	77
8191	31347N	73
8191	30643N	81
8191	32641N	77
8191	33323N	61
8191	37305N	75
8191	37621N	83
8191	30323N	77
8191	30651N	73
8191	37077N	67
8191	365 15N	83
8191	31425N	73
8191	36373N	79
8191	35141N	83
8191	33221N	69
8191	35271N	95
8191	36733N	83
8191	31725N	77
8191	35163N	91
8191	33501N	81
8191	36601N	79
8191	33705N	73
8191	36235N	63
8191	37743N	87
8191	34603N	71
8191	33567N	89
8191	31011N	89
8191	32333N	77
8191	32467N	93
8191	30515N	77

Polynomials of trace 1		
Order	P(x)	MON
8191	35323N	83
8191	34371N	79
8191	34757N	75
8191	37445N	75
8191	36247N	71
8191	32725N	77
8191	34461N	71
8191	35523N	79
8191	35613N	79
8191	36023N	63
8191	32743N	101
8191	34413N	71
8191	33235N	81
8191	32371N	69
8191	31071N	61
8191	31565N	77
8191	30331N	73
8191	34423N	75
8191	32347N	81
8191	33433N	89
8191	30007N	81
8191	31035N	69
8191	37541N	83
8191	33763N	85
8191	33037N	81
8191	34027N	91
8191	37341N	83
8191	34317N	79
8191	30741N	81
8191	30357N	61
8191	35645N	71
8191	34243N	83
8191	37243N	83
8191	32505N	89
8191	33121N	73
8191	32415N	85
8191	31707N	69
8191	37503N	71
8191	36721N	71
8191	32445N	81
8191	33717N	85
8191	36703N	71
8191	33073N	85
8191	3751N	83
8191	34517N	83

Polynomials of trace 1		
Order	P(x)	MON
8191	33631N	77
8191	31627N	73
8191	35351N	79
8191	34131N	67
8191	34655N	91
8191	33405N	81
8191	35543N	79
8191	33507N	69
8191	33255N	77
8191	35147N	79
8191	33057N	85
8191	30755N	89
8191	34407N	71
8191	37017N	67
8191	32635N	77
8191	32563N	93
8191	32115N	81
8191	31457N	81
8191	31743N	81
8191	31123N	73
8191	37767N	67
8191	32275N	73
8191	31145N	69
8191	36203N	71
8191	36037N	95
8191	30561N	73
8191	30543N	77
8191	35165N	71
8191	34063N	87
8191	33165N	77
8191	30465N	73
8191	37213N	71
8191	36455N	91
8191	37335N	71
8191	31535N	77
8191	32437N	85
8191	31113N	73
8191	37603N	75
8191	35325N	71
8191	31671N	73
8191	32311N	77
8191	36753N	79
8191	30117N	77
8191	30171N	89
8191	30277N	65

Polynomials of trace 1		
Order	P(x)	MON
8191	31131N	73
8191	36135N	79
8191	35763N	83
8191	35211N	67
8191	32173N	81
8191	37371N	87
8191	33613N	69
8191	34363N	75
8191	31773N	69
8191	32167N	85
8191	37437N	79
8191	36045N	75
8191	37327N	83
8191	36545N	87
8191	35545N	79
8191	35477N	75
8191	30025N	93
8191	31273N	97
8191	35557N	63
8191	31701N	69
8191	30265N	85
8191	35051N	87
8191	36375N	83
8191	31237N	69
8191	31251N	85
8191	33045N	73
8191	34261N	87
8191	35747N	79
8191	33133N	81
8191	37431N	71
8191	34647N	79
8191	35373N	75
8191	32757N	81
8191	34775N	63
8191	36015N	79
8191	35453N	83
8191	36465N	79
8191	36667N	79
8191	37467N	87
8191	31767N	65
8191	32137N	85
8191	34627N	79
8191	34641N	79
8191	34003N	71
8191	31017N	97

Polynomials of trace 1		
Order	P(x)	MON
8191	36025N	99
8191	36771N	79
8191	35135N	83
8191	34723N	83
8191	32715N	81
8191	32751N	81
8191	35567N	87
8191	32151N	81
8191	30705N	77
8191	3201IN	93
8191	30733N	69
8191	35075N	87
8191	34113N	75
8191	33727N	89
8191	36403N	87
8191	36575N	71
8191	30507N	77
8191	33001N	69
8191	34547N	75
8191	35057N	71
8191	35315N	83
8191	30057N	85
8191	31303N	89
8191	33233N	85
8191	36155N	83
8191	32535N	77
8191	35421N	75
8191	32577N	77
8191	30031N	85
8191	33325N	57
8191	34005N	87
8191	34767N	79
8191	35777N	75
8191	32047N	93
8191	30405N	69
8191	32671N	81
8191	36307N	75
8191	36351N	71
8191	33313N	81
8191	33561N	77
8191	37123N	63
8191	35121N	79
8191	35007N	91
8191	31223N	85
8191	30753N	73

Polynomials of trace I		
Order	P(x)	MON
8191	37475N	83
8191	37033N	71
8191	36551N	71
8191	34713N	91
8191	35455N	67
8191	37011N	75
8191	30417N	89
8191	32731N	81
8191	34047N	87
8191	32033N	73
8191	32517N	77
8191	36427N	91
8191	37521N	87
8191	32245N	97
8191	33625N	73
8191	36625N	71
8191	37653N	67
8191	35631N	79
8191	30763N	77
8191	35465N	91
8191	34151N	71
8191	30301N	57
8191	31267N	73
8191	33721N	97
8191	36463N	79
8191	36217N	75
8191	31047N	81
8191	37053N	79
8191	31407N	65
8191	31333N	85
8191	37415N	91
8191	31653N	85
8191	34273N	79
8191	35673N	75
8191	32555N	69
8191	30147N	73
8191	33441N	85
8191	33163N	77
8191	37101N	79
8191	30573N	81
8191	35561N	83
8191	36073N	83
8191	36661N	71
8191	30177N	81
8191	32223N	81

Polynomials of trace 1		
Order	P(x)	MON
8191	32207N	69
8191	30345N	81
8191	37505N	63
8191	36747N	79
8191	36433N	87
8191	30777N	77
8191	35721N	71
8191	34555N	79
8191	34161N	79
8191	30111N	81
8191	31745N	85
8191	36501N	75
8191	3565 IN	75
8191	31201N	85

Order = Order of the polynomial

P(x)
p(x) expressed in octal terms
MON = Massey-Omura number associate with p(x)