Composite Algorithm: A new algorithm to search for monic irreducible polynomials over extended Galois Field GF(p^q).

Sankhanil Dey[1], Amlan Chakrabarti[2] and Ranjan Ghosh[3],
Department of Radio Physics and Electronics, University of Calcutta,
92 A P C Road, Kolkata-700009[1,3].
and
A K Choudhury School of Information Technology, University of Calcutta,
Sector-III, JD-2 block, Salt Lake City, Kolkata-700098[2].

Email of the Corresponding Author: sankhanil12009@gmail.com or sdrpe_rs@caluniv.ac.in.

Abstract. Irreducible polynomials (IPs) have many applications in the field of computer science and information technology. Algorithms in artificial intelligence and substitution boxes in cryptographic ciphers are some evident example of such important applications. But till now the study is mostly limited to the binary Galois field GF(2^q) where 2 is the modulus and q is the extension of the said Galois field. Some works are there to generate IPs over some non-binary Galois field GF(p^q) where p is the prime modulus and p>2 but the maximum value of p is not more than 13 and the maximum value of extension q is not more than 4. In this paper a new algorithm to search for monic irreducible polynomials over extended Galois field GF(p^q) entitled as " Composite Algorithm" is introduced to computer scientists. Here all possible set of two monic elemental polynomials (EPs)[1] one with highest degree ≤ q-1/2 (for odd value of q) and ≤ q/2 (for even value of q) is multiplied over the Galois field GF(p^q) to one with highest degree ≥ q-1/2 (for odd value of q) and ≥ q/2 (for even value of q). All resultant monic polynomials are then divided over the Galois field GF(p^q) by a monic basic polynomial (BP)[1]. If for all resultant polynomials the residue is 1 for a monic BP then the monic BP is termed as monic IP. The time complexity of the said algorithm is prove to be the best among existing such algorithms and efficient of all among them.

Keywords: Polynomials; Irreducible Polynomials; Algorithms; Numerical Algorithms; Discrete Mathematics;

1. Introduction. IPs over extended Galois fields finds many applications in the modern computer science and information technology. One evident application of the monic IP over Galois field GF(2^8) is the 8-bit substitution box of the Advance Encryption Standard or AES [2][3]. The substitution box of AES constitutes of 2^8 or 64 elements with decimal value 0 to 63 together [2][3]. There are many other applications of IPs over extended Galois fields in modern computer arithmetic and computer applications. Computer algorithm for the generation of monic IPs over the Galois field GF(p^q) for large value of the prime modulus p and the extension q is till now is an unbroken stepping stone in computer science. An algorithm to generate monic reducible polynomials or RPs over the Galois field GF(p^q) [1] through multiplication of monic elemental polynomials or EPs over the Galois field GF(p^q) is already mentioned in [4]. The list of monic IPs over the Galois field GF(p^q) is extracted from the list of all the monic BPs over the Galois field GF(p^q) by the cancellation of all monic RPs over the Galois field GF(p^q) from the list of monic BPs over the Galois field GF(p^q) leaving behind the monic IPs over the Galois field GF(p^q) [4][5]. The multiplication of two monic polynomials over the Galois field GF(p^q) must be according to the multiplication algorithm defined in [6].

Here a new multiplication algorithm is introduced to multiply two monic EPs over the Galois field GF(p^q). The procedure is same as decimal multiplication but the each digit in product must be modulated with prime modulus p to obtain the result. The multiplicand and multiplier are two GFNs of the two monic EPs over the Galois field GF(p^q). The generation of the GFNs [1] is described in section 2.1 and the procedure and the algorithm is described in section 2.2.

In the procedure to subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position of the GFN with small decimal equivalent (DE). If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. A brief description of the procedure of the subtraction of the two Galois field polynomials over the Galois field GF(p^q) and the algorithm for the procedure is detailed in section 2.3.

In the procedure to divide two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient are subtracted from the same number of digits from the most significant bit of the dividend to obtain the residue and the subtraction is made by the procedure defined in section 2.3. The total division procedure and algorithm two Galois field polynomials over the Galois field GF(p^q) is described in sec 2.4.

Now to generate the DEs of all the monic IPs over the Galois field GF(p^q) through composite algorithm here all possible set of two monic elemental polynomials (EPs)[1] one with highest degree ≤ q-1/2 (for odd value of q) and ≤ q/2 (for even value of q) is multiplied over the Galois field GF(p^q) to one with highest degree ≥ q-1/2 (for odd value of q) and ≥ q/2 (for even value of q). All resultant monic polynomials are then divided over the Galois field GF(p^q) by a monic basic polynomial (BP)[1]. If for all resultant polynomials the residue is 1 for a monic BP then the monic BP is termed as monic IP. The procedure and the algorithm for the said algorithm is described in section 3.

The conclusion and acknowledgement of the paper is given in section 4 and section 5 respectively.

2. Related algorithms to generate monic IPs over the Galois field GF(p^q) through Composite Algorithm.

The generation of the GFN is described in subsection 2.1. The procedure and algorithm for the multiplication over the Galois field GF(p^q) of the two GFNs over the said Galois field is illustrated in section 2.2. The procedure and algorithm for the subtraction and division over the Galois field GF(p^q) is described in subsection 2.3 and 2.4 respectively.

2.1. Generation of the GFNs from the Galois field polynomials over the Galois field GF(p^q).

Coefficient of each degree term of a polynomial are arranged sequentially from highest to lowest degree in a decreasing sequence of degree terms (Coefficient of highest degree term is in MSB and coefficient of lowest degree term is in LSB) to obtain Galois Field Numbers (GFNs) for polynomials over the Galois fields GF(p^q) where p is the prime modulus and q is the extension of the said Galois field. There are two special types of GFNs. Binary Coded Numbers or BCN for polynomials over the Galois field GF(2^q) and Finite Field Numbers (FFNs) for polynomials over finite field GF(p^q) where p is non-prime. Examples of some GFNs, BCNs and FFNs are given in table.1, table.2 and table.3 respectively below and the description of the said tables are also given below.

Row	DEs	Polynomials	BCNs
Col→	1	2	3
1	14406	$6x^4$	60000
2	14407	$6x^4+1$	60001
3	2443	x^4+6x	10060
4	2414	x^4+x+6	10016

Table.1. GFNs of four Galois field polynomials over the Galois field GF(7^4).

Row	DEs	Polynomials	BCNs
Col→	1	2	3
1	16	x^4	10000
2	17	x^4+1	10001
3	18	x^4+x	10010
4	19	x^4+x+1	10011
5	20	x^4+x^2	10100

6	21	x^4+x^2+1	10101
7	22	x^4+x^2+x	10110
8	23	x^4+x^2+x+1	10111
9	24	x^4+x^3	11000
A	25	x^4+x^3+1	11001
B	26	x^4+x^3+x	11010
C	27	x^4+x^3+x+1	11011
D	28	$x^4+x^3+x^2$	11100
E	29	$x^4+x^3+x^2+1$	11101
F	30	$x^4+x^3+x^2+x$	11110
G	31	$x^4+x^3+x^2+x+1$	11111

Table.2. BCNs of 16 Galois field polynomials over the Galois field GF(2^4).

Row	**DEs**	**Polynomials**	**BCNs**
Col→	**1**	**2**	**3**
1	768	$3x^4$	30000
2	770	$3x^4+2$	30002
3	264	x^4+2x	10020
4	267	x^4+2x+3	10023

Table.3. FFNs of four Galois field polynomials over the Galois field GF(4^4).

Description of Table.1, Table.2, and Table.3:

Table.1: Examples of four GFNs over the Galois field GF(7^4) are given in row 1 through 4 of Table.1. DEs of the polynomials, the polynomials itself and the respective GFNs are given in column 1, 2 and 3 of the respective rows.

Table.2: Examples of four BCNs over the Galois field GF(2^4) are given in row 1 through 16 of Table.2. DEs of the polynomials, the polynomials itself and the respective BCNs are given in column 1, 2 and 3 of the respective rows.

Table.3: Examples of four FFNs over the Galois field GF(4^4) are given in row 1 through 4 of Table.3. DEs of the polynomials, the polynomials itself and the respective FFNs are given in column 1, 2 and 3 of the respective rows.

2.2 Procedure and the algorithm for multiplication of the two BCNs over the Galois field GF(p^q).

Here a new multiplication algorithm is introduced to multiply two monic EPs over the Galois field GF(p^q). The procedure is same as decimal multiplication but the each digit in product must be modulated with prime modulus p to obtain the result. The multiplicand and multiplier are two GFNs of the two monic EPs over the Galois field GF(p^q). The procedure is introduced in subsection 2.2.1 and subsection 2.2 is dedicated to algorithm of the said procedure.

2.2.1 Procedure. Let us consider two EPs over Galois field GF(2^4), multiplication of those two EPs over Galois field GF(2^4) must construct a BP. Two EPs over Galois field GF(2^4) are,

EPs	**BCNs or GFNs**
x	0010
x^3+1	1001

Polynomial multiplication of concerned two EPs over Galois field GF(2^4)**:** $x.(x^3+1) = x^4+x$ (BCN = 10010).

Now, by BCNs

A. 1st number. 0010

B. 2nd number. 1001

```
          0010
         0000
        0000
       0010
Product.  0-0-1-0-0-1-0
```

```
 %-%-%-%-%
 2-2-2-2-2
 --------------
 1-0-0-1-0
```

Product BP = BCN or GFN = 10010 = **polynomial =** x^4+x = Decimal Equivalent = 18.

2.2.2 Algorithm.

The algorithm of multiplication of two polynomials over the Galois field GF(2^4) is given as follows,

Start.

Step 0. Let us take DE of two polynomials A and B over Galois field GF(2^4).

Step 1. Convert two numbers into two BCNs, BCN(A) and BCN(B).

Step 2. Multiply BCN(A) and BCN(B) with decimal multiplication to obtain product P(A×B).

Step 4. Modulate each digit of product with 2 two obtain product BCN of P(A×B).

Stop.

2.3 Procedure and the algorithm for subtraction of the two BCNs over the Galois field GF(p^q).

To subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position GFN with small decimal equivalent (DE) and modulate with p. If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. A brief description of the procedure of the subtraction of the two Galois field polynomials over the Galois field GF(p^q) is given in subsection 2.3.1 and the algorithm for the procedure is detailed in section 2.3.2.

2.3.1 Procedure:

To subtract two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials and subtract each corresponding digit of the GFN with small decimal equivalent (DE) from the GFN with large DE and modulate the result with p to obtain the corresponding subtracted digit. If the subtracted digit is negative then add p as borrow to the next position GFN with small decimal equivalent (DE) and modulate with p. If two GFNs have unequal numbers of digits then pad the GFN with small decimal equivalent (DE) with 0s in left. Example for two BCNs and two GFNs are given below,

Key Definitions.

Basic polynomials (BPs) over Galois field GF(2^4). Polynomials over the Galois field GF(2^4) with highest degree 4 are termed as BPs over Galois field GF(2^4).

Elemental polynomials (EPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with highest degree less than 4 are termed as EPs over Galois field GF(2^4).

Binary Coded Numbers (BCNs) or Galois field Numbers (GFNs) over Galois field GF(2^4). If it is considered that coefficient of highest degree term of the concerned polynomial is the MSB of the number and coefficient of lowest degree term of the concerned polynomial is the LSB of the number and other coefficients of highest degree to lowest degree term are arranged sequentially from MSB to LSB in the number then the number constructed with coefficients of the concerned polynomial is termed as BCN or which is also a GFN over Galois field GF(2^4).

Subtraction of two BCNs over Galois field GF(2^4):

Two EPs over Galois field GF(2^4) are,

EPs	**BCNs or GFNs**
x	0010
x^3+1	1001

Now,

BCN(x) < BCN(x^3+1). If we subtract BCN(x) from BCN(x^3+1) we get, subtract in decimal each digit of BCN(x) from BCN(x^3+1) and modulate the result with 2 when result is negative add borrow 1 to next position of the BCN(x) and modulate with 2.

A. **1-0-0-1**

B. **0-0-1-0**

Difference. 0-1-1-1

2.3.2 Algorithm:

The algorithm is given below,

Start.

Step 1: The four bits of the 1st BCN or BCN(x^3+1) with greater value of DE are stored at bcn_large.bit0, bcn_large.bit1, bcn_large.bit2, bcn_large.bit3 from MSB to LSB respectively and The four bits of the 2nd BCN or BCN(x) with smaller value of DE are stored at bcn_small.bit0, bcn_small.bit1, bcn_small.bit2, bcn_small.bit3 from MSB to LSB respectively.

Step 2: The subtraction is started from LSB.

Step 3: bcn_small.bit3 is subtracted from bcn_large.bit3 and the obtained digit is modulated with 2. If the result is negative then add borrow 1 to the bcn_small.bit2 and subtract it from bcn_large.bit2 and modulate the obtained digit with 2 to obtain the 2nd subtracted digit of the difference. The procedure is going on till the subtraction of bcn_small.bit0 from bcn_large.bit0.

Step 4: The obtained four corresponding digits are stored in diff.bit0, diff.bit1, diff.bit2 and diff.bit3 respectively.

Stop.

2.4 Procedure and the algorithm for division of the two BCNs over the Galois field GF(p^q).

To divide two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient are subtracted from the same number of digits from most significant bit of the dividend to obtain the residue and the subtraction is made by the procedure defined in section 2.3. The total division procedure is given in subsection 2.4.1 and the algorithm to divide two Galois field polynomials over the Galois field GF(2^4) is described in subsection 2.4.2.

2.4.1 Procedure.

In division of the two Galois field polynomials over the Galois field GF(p^q) generate the GFNs [1] of the two said polynomials at first. Division over the Galois field GF(p^q) procedure is same as decimal division but there are some important modifications in this division procedure. The product of divisor and each digit of quotient are subtracted from the same number of digits from most significant bit of the dividend to obtain the residue and the subtraction is made by the procedure defined in section 3.2. The procedure for the two GFNs more specifically for the two BCNs is as follows,

Two Polynomials over the Galois field GF(2^4) are,

Polynomials	**BCNs or GFNs**
x	0010
x^3+1	1001

Now,

BCN(x) < BCN(x^3+1). The division of the BCN(x^3+1) by BCN(x) would result as follows,

```
10)1001(100
    10
   ------------
    000
     00
   ------------
     01
     00
 --------------
      1
```

In this division the division is similar to decimal division but the subtraction is according to subtraction of two BCNs over Galois field GF(2^4).

2.4.2 Algorithm.

The algorithm for the division of the two BCNs over the Galois field $GF(2^4)$ is given below,

Start.

Step 0. Let us take the DEs of the two polynomials A and B over Galois field $GF(2^4)$.

Step 1. Convert the two numbers into two BCNs, BCN(A) and BCN(B).

Step 2. If **(**BCN(A)>BCN(B) then [avoid zero padding],

Step 3. divide BCN(A) by BCN(B) with decimal division to obtain quotient D(A/B) and residue R(A/B) but the only difference is the subtraction used in division is according to subtraction of two BCNs over Galois field $GF(2^4)$.

Stop.

3. Composite Algorithm.

The procedure of the algorithm is described in subsection 3.1. The algorithm for the Galois field $GF(p^q)$ is described in subsection 3.2.

3.1 Procedure.

Now to generate the DEs of all the monic IPs over the Galois field $GF(p^q)$ through composite algorithm here all possible set of two monic elemental polynomials (EPs)[1] one with highest degree $\leq$ q-1/2 (for odd value of q) and $\leq$ q/2 (for even value of q) is multiplied over the Galois field $GF(p^q)$ to one with highest degree $\geq$ q-1/2 (for odd value of q) and $\geq$ q/2 (for even value of q). All resultant monic polynomials are then divided over the Galois field $GF(p^q)$ by a monic basic polynomial (BP)[1]. If for all resultant polynomials the residue is 1 for a monic BP then the monic BP is termed as monic IP.

3.2 Algorithm for the Galois field $GF(p^q)$.

Let us consider monic BPs, BP over extended Galois field $GF(p^q)$ with degree BPD €q and consider monic EPs, EP with degree EPD € {1,2,…..,(q-1)/2}. Since monic EPs with degree d and q-d can be the MIs of each other so the division is restricted to the aforesaid condition. Now let the total number of monic BPs over the Galois field $GF(p^q)$ have been p^q € n and monic EPs over the Galois field $GF(p^q)$ (p^q-p) € n-p;

```
Start.
BP_Numbers: n; // Defining total numbers of monic BPs to be tested to be a monic IP.
EP_Numbers: n-p;  // Defining total numbers of monic EPs.
For BP_index::1: n.     // Accessing each monic BP.
      For EP_index::1: n-p.   // Access to each monic EP.
// Testing of Boundary Condition for a Monic BP to be a Monic IP
            If ((EP1×EP2) %(GF) (BP) == 1)
                  Flag [EP_index]=1;
            End If.
      End For (EP_index)      // End of For loop EP_index.
      If (Flag [EP_index]==1) for all EPs
            BP= IP. // Declaration of a Monic BP to a Monic IP.
       Else BP = RP. // Declaration of a Monic BP to a Monic RP.
End For (BP_index.)      // End of For loop BP_index.
Stop.
```

Note: Time complexity of Composite Algorithm is $O(n^2)$.

3.3 Comparison of time complexity of the given algorithm with Rabin's Algorithms.

The new composite algorithm to find the monic IPs over Galois field GF(p^q) have a time complexity of O(n^2). Since time complexity of Rabin's algorithm and its modification depends upon the value of prime modulus p so it becomes slower for large value of p. Now in this algorithm the complexity depends upon the value of extension q so they are faster and eligible to find monic IPs for very large value of p as well as extension q.

Algorithms	**Composite Algorithm**	**Rabin's Algorithm**	**Rabin's Algorithm(mod)**
Time Complexity	$O(n^2)$	$O(n^4(\log P)^3)$	$0(n^4(\log p)^2 + n^3(\log P)^3)$

Table.4. Comparison of Time Complexity of the division algorithm with Rabin's and Modified Rabin's Algorithm.

4. Conclusion. From the last few decades computer scientists try to break the untouched stone of the composite algorithm to reduce the time complexity of many algorithms in computer science and artificial intelligence. In this paper this stone is broken to find the large numbers of monic IPs over the extended Galois field GF(p^q) where prime modulus p is very large with a very large value of extension q. The algorithm reduces the required time almost 100 times rather than the previous algorithms and the excellence of the algorithm is also increased for 100 times than the previous ones. The time complexity analysis proves the previous statements true and the composite algorithm to be the best algorithm ever to find the large numbers of monic IPs over the extended Galois field GF(p^q) where prime modulus p is very large with a very large value of extension q.

5. Acknowledgements. I would like to acknowledge Prof. (Dr.) Gopa Sen, Head Dept. Radio Physics and Electronics of the University of Calcutta and Prof. Amlan Chakrabarti, Director of the A K Choudhury School of Information Technology of the University of Calcutta for providing me the uninterrupted infrastructure to carry out the research. I would also like to thank TEQIP-Phase-II for providing me the financial support up to 30th November 2016.

References.

1. Sankhanil Dey, Amlan Chakrabarti , Ranjan Ghosh . (2019) 4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(2^4) and cryptanalysis., International Journal of Tomography and Simulation, ISSN: 2319-3336, Vol. 32, Issue No. 3, CESER publication.

2. Sankhanil Dey and Ranjan Ghosh (2018)"A smart review and two new techniques using 4-bit Boolean functions for cryptanalysis of 4-bit crypto S-boxes.", Vol.40, issue.3, pp.1-19, International Journal of Computers and Applications, Taylor and Francis publishers, ISSN. 1206-212X. DOI. **https://doi.org/10.1080/1206212X.2018.1504459**.

3. Joan Daemen,Vincent Rijmen (2000), AES Proposal: Rijndael,http://csrc.nist.gov/encryption/aes/ Last Visited: 7th February 2001.

4. Church R, Tables of irreducible polynomials for the first four prime moduli, The Annals of Maths., 2nd Series, vol. 36, no. 1, 198-209, Jan (1935) http://www.jstor.org/stable/1968675.

5. Sankhanil Dey and Ranjan Ghosh, (2017) A new mathematical method to search irreducible polynomials using decimal equivalents of polynomials over Galois field GF(p^q), Journal: Circulation in Computer Science, Vol.2, No.11. pp-17-22, CSL Press, New York, DOI, ISSN. 2456-3692. **https://doi.org/10.22632/ccs-2017-252-68**.

6. Sankhanil Dey. and Ranjan Ghosh. (2018) Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field GF(p^q). Open Journal of Discrete Mathematics, Scientific Research Publishers, 8 (1), 21-33, ISSN online. 2161-7643 ISSN online. 2161-7635. **https://doi.org/10.4236/ojdm.2018.81003**.