Appendices - 3

Jayati dutta

October 3, 2024

1 Possible Polynomials of order 8

Table 1: Summary of the best cases of each Irreducible Polynomials

Poly no.	Irreducible Polynomial	Practical NL	DU	Bijectivity
1	$x^8+x^4+x^3+x+1$	102	8	yes
2	$x^8+x^6+x^3+x^2+1$	100	8	yes
3	$x^8+x^6+x^4+x^3+x^2+x+1$	100	8	yes
4	$x^8+x^6+x^5+x+1$	102	8	yes
5	$x^8+x^6+x^5+x^2+1$	102	8	yes
6	$x^8+x^6+x^5+x^3+1$	102	8	yes
7	$x^8+x^7+x^3+x^2+1$	110	8	yes
8	$x^8+x^7+x^6+x+1$	102	8	yes
9	$x^8+x^7+x^6+x^5+x^4+x^2+1$	110	8	yes
10	$x^8+x^5+x^4+x^3+1$	100	8	yes
11	$x^8+x^5+x^4+x^3+x^2+x+1$	104	8	yes
12	$x^8+x^6+x^5+x^4+x^2+x+1$	100	8	yes
13	$x^8+x^7+x^4+x^3+x^2+x+1$	102	8	yes
14	$x^8+x^7+x^5+x+1$	102	8	yes
15	$x^8+x^7+x^5+x^3+1$	102	8	yes
16	$x^8+x^7+x^6+x^5+x^4+x^3+1$	102	8	yes
17	$x^8+x^4+x^3+x^2+1$	98	8	yes
18	$x^8+x^5+x^3+x+1$	101	8	yes
19	$x^8+x^5+x^3+x^2+1$	103	8	yes
20	$x^8+x^6+x^5+x^4+1$	99	8	yes
21	$x^8+x^6+x^5+x^4+x^3+x+1$	98	8	yes
22	$x^8+x^7+x^2+x+1$	101	8	yes
23	$x^8+x^7+x^3+x+1$	101	8	yes
24	$x^8+x^7+x^5+x^4+1$	99	8	yes
25	$x^8+x^7+x^5+x^4+x^3+x^2+1$	101	8	yes
26	$x^8+x^7+x^6+x^3+x^2+x+1$	99	8	yes
27	$x^8+x^7+x^6+x^4+x^2+x+1$	4	130	yes
28	$x^8+x^7+x^6+x^4+x^3+x^2+1$	98	8	yes
29	$x^8+x^7+x^6+x^5+x^2+x+1$	103	8	yes
30	$x^8+x^7+x^6+x^5+x^4+x+1$	101	8	yes

2 Algorithms

Algorithm 1 Finding Multiplicative Inverses

procedure FINDINVERSE(p, irreducible_poly)
  Input: p, an element for which we are finding the inverse.
  Output: q, such that $p \times q = 1$ mod irreducible_poly
  Initialize $q = 0$.
  for $q = 0$ to FF **do**
    if (p × q) mod irreducible_poly == 1 **then**
      Return q as the multiplicative inverse.
  If no such q exists, report that p has no multiplicative inverse.

Algorithm 2 Proposed Algorithm for Fixing $\vec{M}$

procedure PROCEDURE-3
  Generate an array of size 8 using 0 and 1.
  Initially, the array contains one 1 and the rest are 0s.
  Generate a Circulant matrix using this array.
  for $i = 1$ to 8 **do**
    Increase the number of 1s in the array.
    Generate all possible combinations of 0 and 1.

Algorithm 3 Proposed Algorithm for Fixing $\vec{b}$

procedure PROCEDURE-4
  Generate an array of size 8 using 0 and 1.
  Initially, the array contains all 0s.
  for $i = 1$ to 8 **do**
    Increase the number of 1s in the array.
    Generate all possible combinations of 0 and 1.