Multiplication in Finite Fields of Characteristic 2

Guillermo Morales-Luna
Computer Science Section
CINVESTAV-IPN, Mexico
gmorales@cs.cinvestav.mx

February 18, 2010

Abstract

Using a canonical enumeration procedure, we identify each Galois field of characteristic 2 with the corresponding integer interval with extremes 0 and the corresponding Marsenne number. We plot the graphs of the field operations through that identification.

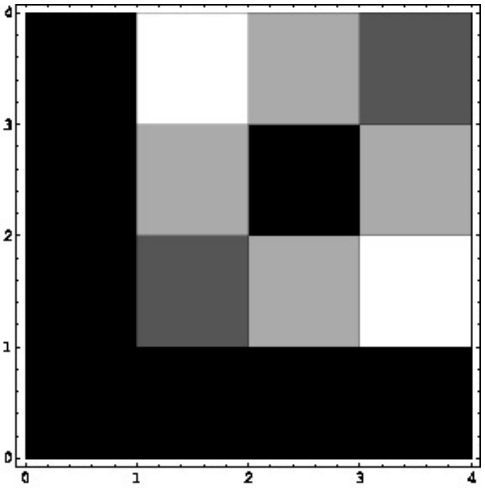
Contents

1 Introduction

The Galois fields of characteristic 2 have been widely used in technological applications, mainly in Coding Theory and Cryptography. Each Galois field of characteristic 2, let us say of degree n, has as cardinality the corresponding power of 2, and its elements are representable by n-degree polynomials, thus the Galois field can be identified with the set of integers with extrems 0 and $2^n - 1$. In this document we translate the operations in the Galois field into that integer interval and we plot as density graphs the translated operations, just to give a global glimpse of the field operations. All graphs were obtained using `Mathematica 3.0`. All concepts mentioned here can be explored more deeply in the classical text of Lidl and Niederreiter [1].

0	0	0	0
0	1	2	3
0	2	0	2
0	3	2	1

(a)



(b)

Table 1: Ring multiplication table in the modulus ring $[\![0, 2^2 - 1]\!]$.

2 Ring multiplication

The set $[\![0, 2^n - 1]\!]$ consists of the collection of remainders modulus 2^n. It has naturally the ring multiplication operation $(i, j) \mapsto (ij) \bmod 2^n$. These operations are displayed in tables 1-5 for $n \leq 5$. In each display, table (a) contains the numeric values, and, as is usual when displaying matrices, its rows are numbered from up to bottom; the corresponding graphical table (b) displays the same operation in a scale of gray: black color corresponds to the lowest value 0 while white color corresponds to the greatest value $2^n - 1$; this time the rows are numbered from bottom to up.

3 Representation of Galois fields of characteristic 2

Let $\mathbb{F}_2 = \{0, 1\}$ be the *prime Galois field* consisting of just two elements. For most integer values $n \geq 2$ there is a minimum k, with $0 < k < n$, such that the polynomial $p_{nk}(X) = X^n + X^k + 1$ is irreducible over the field $\mathbb{F}_2$. In Table 6 we display such pairs $(n : k)$, for $n = 2, \ldots, 101$. The cases in which there is no such k are distinguished by making $k = n$, in them any irreducible polynomial of degree n shall involve more than one intermediate powers X^k. Whenever $p_{nk}(X)$ is irreducible, the Galois field $\mathbb{F}_{2^n}$ is isomorphic to the quotient $\mathbb{F}_2[X]/(p_{nk}(X))$, and, consequently, the arithmetic in the field can be realized as the polynomial arithmetic reduced modulus $p_{nk}(X)$. Each element in $\mathbb{F}_{2^n}$ is of the form $p_{\boldsymbol{\epsilon}}(X) = \sum_{i=1}^{n} \epsilon_i X^{i-1}$ and is naturally identified with the integer $I_{\boldsymbol{\epsilon}} = \sum_{i=1}^{n} \epsilon_i 2^{i-1} \in [\![0, 2^n - 1]\!]$.

4 Field operations with the polynomial representation

4.1 Multiplication

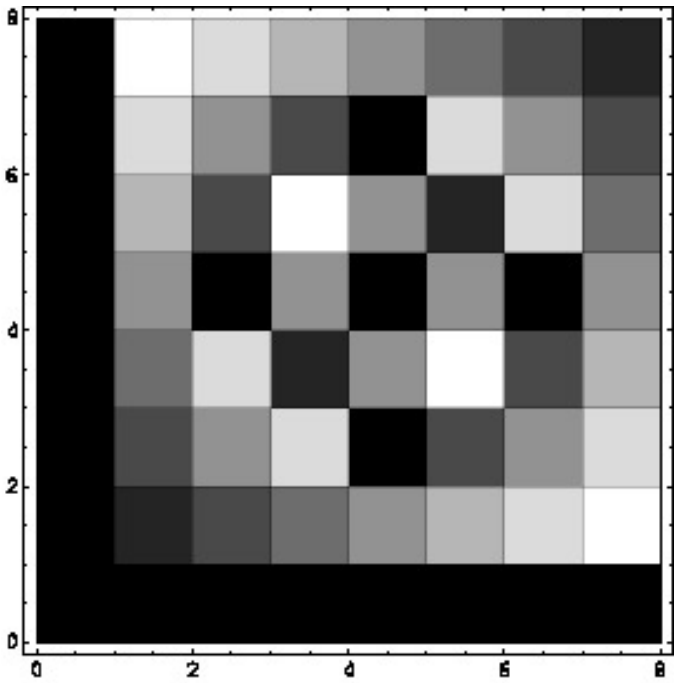
The field multiplication determines the operation

$$\star : [\![0, 2^n - 1]\!] \times [\![0, 2^n - 1]\!] \to [\![0, 2^n - 1]\!] \ , \ (I_{\boldsymbol{\epsilon}}, I_{\boldsymbol{\delta}}) \mapsto I_{\boldsymbol{\gamma}},$$

where the vector index $\boldsymbol{\gamma}$ is such that $p_{\boldsymbol{\gamma}}(X) = p_{\boldsymbol{\epsilon}}(X) p_{\boldsymbol{\delta}}(X)$. In tables 7-11 these operations are displayed for $n = 2, 3, 4, 5$ respectively.

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	2	4	6	0	2	4	6
0	3	6	1	4	7	2	5
0	4	0	4	0	4	0	4
0	5	2	7	4	1	6	3
0	6	4	2	0	6	4	2
0	7	6	5	4	3	2	1

(a)

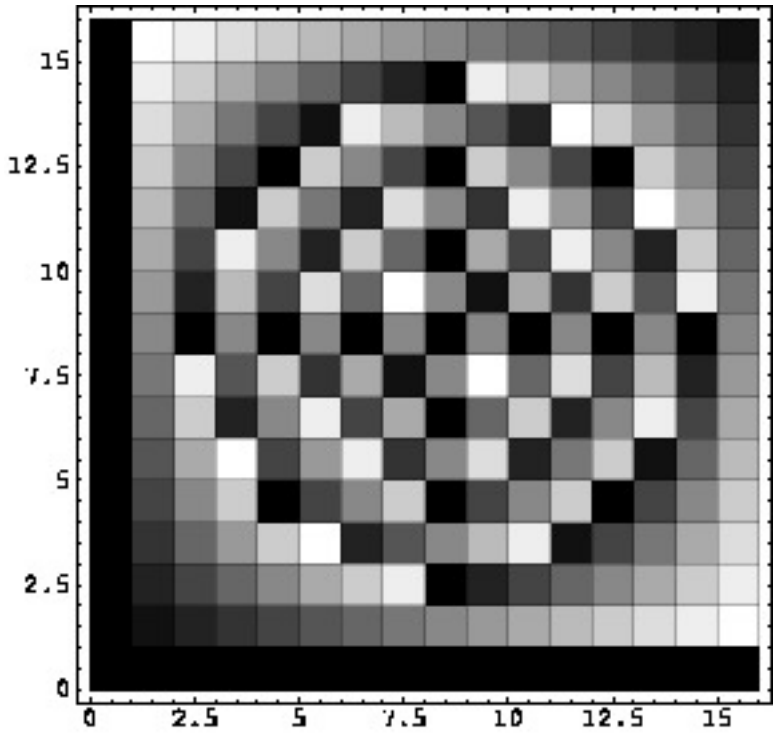


(b)

Table 2: Ring multiplication table in the modulus ring $[\![0, 2^3 - 1]\!]$.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	4	6	8	10	12	14	0	2	4	6	8	10	12	14
0	3	6	9	12	15	2	5	8	11	14	1	4	7	10	13
0	4	8	12	0	4	8	12	0	4	8	12	0	4	8	12
0	5	10	15	4	9	14	3	8	13	2	7	12	1	6	11
0	6	12	2	8	14	4	10	0	6	12	2	8	14	4	10
0	7	14	5	12	3	10	1	8	15	6	13	4	11	2	9
0	8	0	8	0	8	0	8	0	8	0	8	0	8	0	8
0	9	2	11	4	13	6	15	8	1	10	3	12	5	14	7
0	10	4	14	8	2	12	6	0	10	4	14	8	2	12	6
0	11	6	1	12	7	2	13	8	3	14	9	4	15	10	5
0	12	8	4	0	12	8	4	0	12	8	4	0	12	8	4
0	13	10	7	4	1	14	11	8	5	2	15	12	9	6	3
0	14	12	10	8	6	4	2	0	14	12	10	8	6	4	2
0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

(a)



(b)

Table 3: Ring multiplication table in the modulus ring $[\![0, 2^4 - 1]\!]$.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
0	3	6	9	12	15	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11	14	17	20	23	26	29
0	4	8	12	16	20	24	28	0	4	8	12	16	20	24	28	0	4	8	12	16	20	24	28	0	4	8	12	16	20	24	28
0	5	10	15	20	25	30	3	8	13	18	23	28	1	6	11	16	21	26	31	4	9	14	19	24	29	2	7	12	17	22	27
0	6	12	18	24	30	4	10	16	22	28	2	8	14	20	26	0	6	12	18	24	30	4	10	16	22	28	2	8	14	20	26
0	7	14	21	28	3	10	17	24	31	6	13	20	27	2	9	16	23	30	5	12	19	26	1	8	15	22	29	4	11	18	25
0	8	16	24	0	8	16	24	0	8	16	24	0	8	16	24	0	8	16	24	0	8	16	24	0	8	16	24	0	8	16	24
0	9	18	27	4	13	22	31	8	17	26	3	12	21	30	7	16	25	2	11	20	29	6	15	24	1	10	19	28	5	14	23
0	10	20	30	8	18	28	6	16	26	4	14	24	2	12	22	0	10	20	30	8	18	28	6	16	26	4	14	24	2	12	22
0	11	22	1	12	23	2	13	24	3	14	25	4	15	26	5	16	27	6	17	28	7	18	29	8	19	30	9	20	31	10	21
0	12	24	4	16	28	8	20	0	12	24	4	16	28	8	20	0	12	24	4	16	28	8	20	0	12	24	4	16	28	8	20
0	13	26	7	20	1	14	27	8	21	2	15	28	9	22	3	16	29	10	23	4	17	30	11	24	5	18	31	12	25	6	19
0	14	28	10	24	6	20	2	16	30	12	26	8	22	4	18	0	14	28	10	24	6	20	2	16	30	12	26	8	22	4	18
0	15	30	13	28	11	26	9	24	7	22	5	20	3	18	1	16	31	14	29	12	27	10	25	8	23	6	21	4	19	2	17
0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16	0	16
0	17	2	19	4	21	6	23	8	25	10	27	12	29	14	31	16	1	18	3	20	5	22	7	24	9	26	11	28	13	30	15
0	18	4	22	8	26	12	30	16	2	20	6	24	10	28	14	0	18	4	22	8	26	12	30	16	2	20	6	24	10	28	14
0	19	6	25	12	31	18	5	24	11	30	17	4	23	10	29	16	3	22	9	28	15	2	21	8	27	14	1	20	7	26	13
0	20	8	28	16	4	24	12	0	20	8	28	16	4	24	12	0	20	8	28	16	4	24	12	0	20	8	28	16	4	24	12
0	21	10	31	20	9	30	19	8	29	18	7	28	17	6	27	16	5	26	15	4	25	14	3	24	13	2	23	12	1	22	11
0	22	12	2	24	14	4	26	16	6	28	18	8	30	20	10	0	22	12	2	24	14	4	26	16	6	28	18	8	30	20	10
0	23	14	5	28	19	10	1	24	15	6	29	20	11	2	25	16	7	30	21	12	3	26	17	8	31	22	13	4	27	18	9
0	24	16	8	0	24	16	8	0	24	16	8	0	24	16	8	0	24	16	8	0	24	16	8	0	24	16	8	0	24	16	8
0	25	18	11	4	29	22	15	8	1	26	19	12	5	30	23	16	9	2	27	20	13	6	31	24	17	10	3	28	21	14	7
0	26	20	14	8	2	28	22	16	10	4	30	24	18	12	6	0	26	20	14	8	2	28	22	16	10	4	30	24	18	12	6
0	27	22	17	12	7	2	29	24	19	14	9	4	31	26	21	16	11	6	1	28	23	18	13	8	3	30	25	20	15	10	5
0	28	24	20	16	12	8	4	0	28	24	20	16	12	8	4	0	28	24	20	16	12	8	4	0	28	24	20	16	12	8	4
0	29	26	23	20	17	14	11	8	5	2	31	28	25	22	19	16	13	10	7	4	1	30	27	24	21	18	15	12	9	6	3
0	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2	0	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
0	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table 4: Ring multiplication table in the modulus ring $[\![0, 2^5 - 1]\!]$ (numerical values).

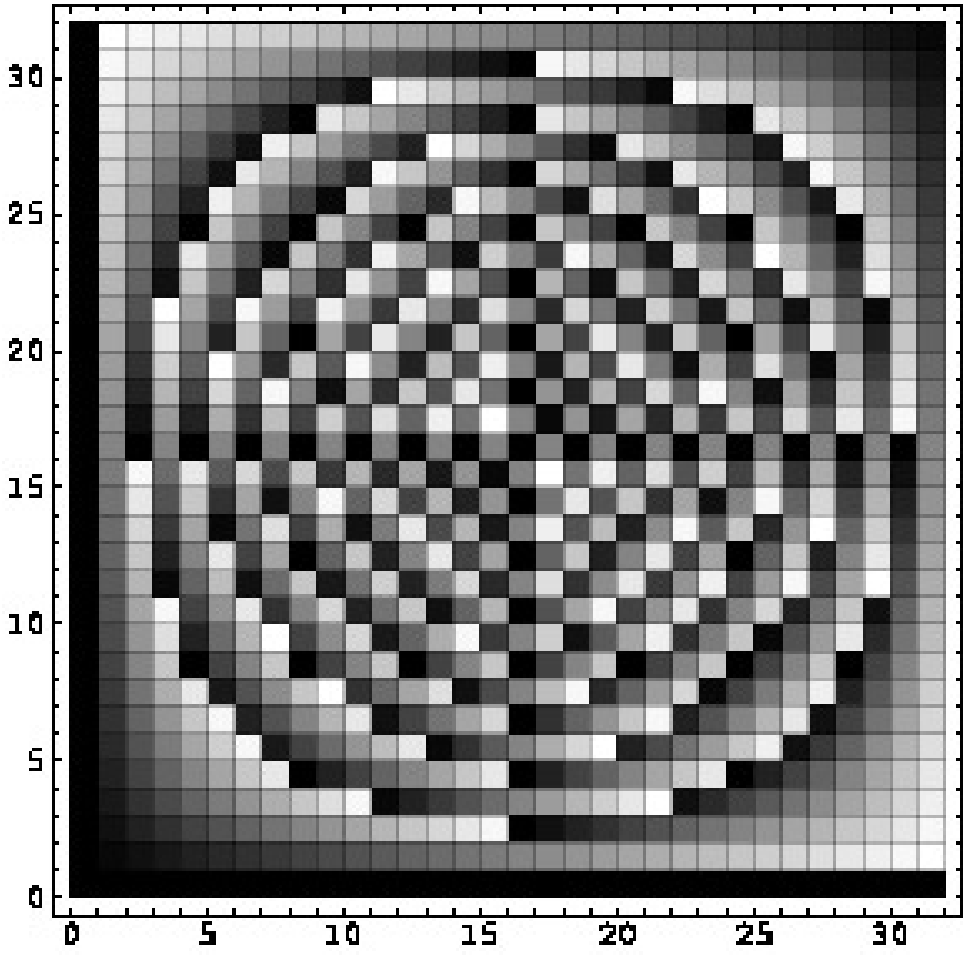


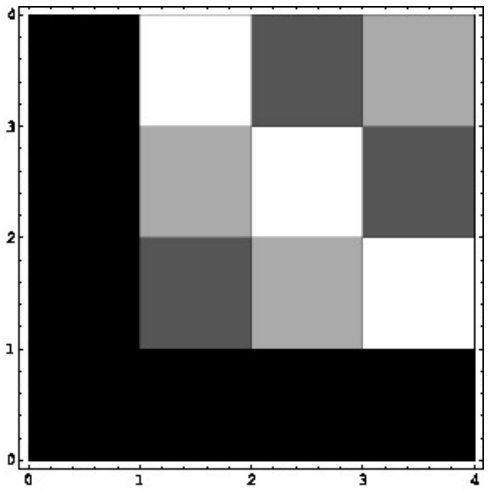
Table 5: Ring multiplication table in the modulus ring $[\![0, 2^5 - 1]\!]$ (density plot).

(2 : 1)	(3 : 1)	(4 : 1)	(5 : 2)	(6 : 1)	(7 : 1)	(8 : 2)	(9 : 1)	(10 : 3)	(11 : 2)
(12 : 2)	(13 : 13)	(14 : 2)	(15 : 1)	(16 : 4)	(17 : 3)	(18 : 2)	(19 : 19)	(20 : 3)	(21 : 2)
(22 : 1)	(23 : 5)	(24 : 4)	(25 : 3)	(26 : 26)	(27 : 27)	(28 : 1)	(29 : 2)	(30 : 1)	(31 : 3)
(32 : 8)	(33 : 10)	(34 : 6)	(35 : 2)	(36 : 4)	(37 : 37)	(38 : 38)	(39 : 4)	(40 : 6)	(41 : 3)
(42 : 4)	(43 : 43)	(44 : 2)	(45 : 45)	(46 : 1)	(47 : 5)	(48 : 8)	(49 : 9)	(50 : 6)	(51 : 51)
(52 : 3)	(53 : 53)	(54 : 9)	(55 : 7)	(56 : 2)	(57 : 4)	(58 : 4)	(59 : 59)	(60 : 1)	(61 : 61)
(62 : 6)	(63 : 1)	(64 : 16)	(65 : 18)	(66 : 3)	(67 : 67)	(68 : 9)	(69 : 69)	(70 : 4)	(71 : 6)
(72 : 8)	(73 : 25)	(74 : 35)	(75 : 75)	(76 : 21)	(77 : 77)	(78 : 8)	(79 : 9)	(80 : 12)	(81 : 4)
(82 : 6)	(83 : 83)	(84 : 5)	(85 : 85)	(86 : 21)	(87 : 13)	(88 : 4)	(89 : 38)	(90 : 27)	(91 : 91)
(92 : 2)	(93 : 2)	(94 : 10)	(95 : 11)	(96 : 16)	(97 : 6)	(98 : 11)	(99 : 99)	(100 : 12)	(101 : 101)

Table 6: Pairs $(n : k)$ such that $p_{nk}(X) = X^n + X^k + 1$ is an irreducible polynomial over the field $\mathbb{F}_2$.

0	0	0	0
0	1	2	3
0	2	3	1
0	3	1	2

(a)

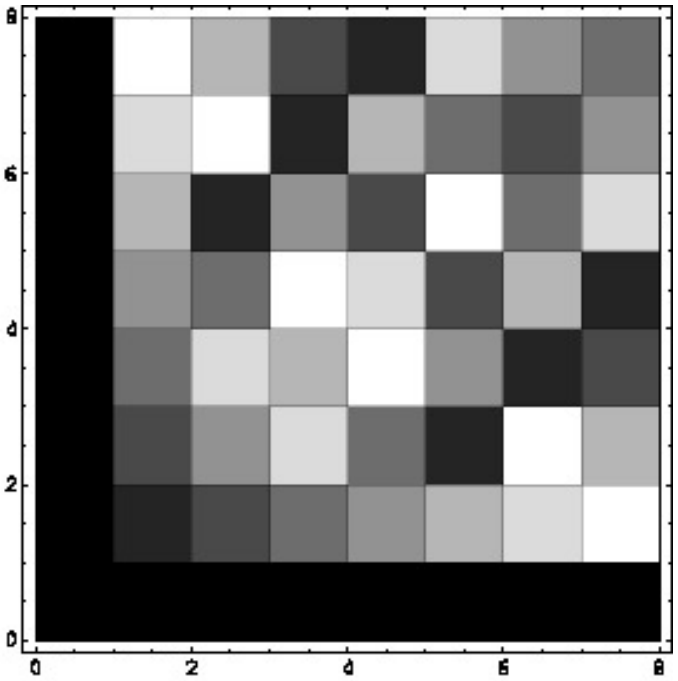


(b)

Table 7: Multiplication table in the Galois field $\mathbb{F}_{2^2}$.

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	2	4	6	3	1	7	5
0	3	6	5	7	4	1	2
0	4	3	7	6	2	5	1
0	5	1	4	2	7	3	6
0	6	7	1	5	3	2	4
0	7	5	2	1	6	4	3

(a)

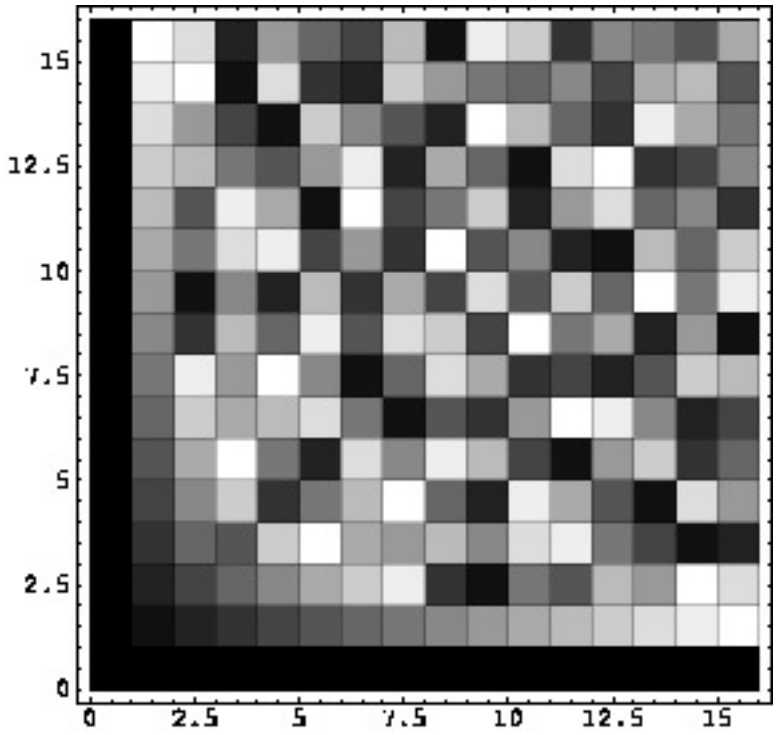


(b)

Table 8: Multiplication table in the Galois field $\mathbb{F}_{2^3}$.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
0	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
0	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
0	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
0	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
0	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
0	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
0	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
0	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
0	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
0	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
0	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
0	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

(a)



(b)

Table 9: Multiplication table in the Galois field $\mathbb{F}_{2^4}$.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	5	7	1	3	13	15	9	11	21	23	17	19	29	31	25	27
0	3	6	5	12	15	10	9	24	27	30	29	20	23	18	17	21	22	19	16	25	26	31	28	13	14	11	8	1	2	7	4
0	4	8	12	16	20	24	28	5	1	13	9	21	17	29	25	10	14	2	6	26	30	18	22	15	11	7	3	31	27	23	19
0	5	10	15	20	17	30	27	13	8	7	2	25	28	19	22	26	31	16	21	14	11	4	1	23	18	29	24	3	6	9	12
0	6	12	10	24	30	20	18	21	19	25	31	13	11	1	7	15	9	3	5	23	17	27	29	26	28	22	16	2	4	14	8
0	7	14	9	28	27	18	21	29	26	19	20	1	6	15	8	31	24	17	22	3	4	13	10	2	5	12	11	30	25	16	23
0	8	16	24	5	13	21	29	10	2	26	18	15	7	31	23	20	28	4	12	17	25	1	9	30	22	14	6	27	19	11	3
0	9	18	27	1	8	19	26	2	11	16	25	3	10	17	24	4	13	22	31	5	12	23	30	6	15	20	29	7	14	21	28
0	10	20	30	13	7	25	19	26	16	14	4	23	29	3	9	17	27	5	15	28	22	8	2	11	1	31	21	6	12	18	24
0	11	22	29	9	2	31	20	18	25	4	15	27	16	13	6	1	10	23	28	8	3	30	21	19	24	5	14	26	17	12	7
0	12	24	20	21	25	13	1	15	3	23	27	26	22	2	14	30	18	6	10	11	7	19	31	17	29	9	5	4	8	28	16
0	13	26	23	17	28	11	6	7	10	29	16	22	27	12	1	14	3	20	25	31	18	5	8	9	4	19	30	24	21	2	15
0	14	28	18	29	19	1	15	31	17	3	13	2	12	30	16	27	21	7	9	6	8	26	20	4	10	24	22	25	23	5	11
0	15	30	17	25	22	7	8	23	24	9	6	14	1	16	31	11	4	21	26	18	29	12	3	28	19	2	13	5	10	27	20
0	16	5	21	10	26	15	31	20	4	17	1	30	14	27	11	13	29	8	24	7	23	2	18	25	9	28	12	19	3	22	6
0	17	7	22	14	31	9	24	28	13	27	10	18	3	21	4	29	12	26	11	19	2	20	5	1	16	6	23	15	30	8	25
0	18	1	19	2	16	3	17	4	22	5	23	6	20	7	21	8	26	9	27	10	24	11	25	12	30	13	31	14	28	15	29
0	19	3	16	6	21	5	22	12	31	15	28	10	25	9	26	24	11	27	8	30	13	29	14	20	7	23	4	18	1	17	2
0	20	13	25	26	14	23	3	17	5	28	8	11	31	6	18	7	19	10	30	29	9	16	4	22	2	27	15	12	24	1	21
0	21	15	26	30	11	17	4	25	12	22	3	7	18	8	29	23	2	24	13	9	28	6	19	14	27	1	20	16	5	31	10
0	22	9	31	18	4	27	13	1	23	8	30	19	5	26	12	2	20	11	29	16	6	25	15	3	21	10	28	17	7	24	14
0	23	11	28	22	1	29	10	9	30	2	21	31	8	20	3	18	5	25	14	4	19	15	24	27	12	16	7	13	26	6	17
0	24	21	13	15	23	26	2	30	6	11	19	17	9	4	28	25	1	12	20	22	14	3	27	7	31	18	10	8	16	29	5
0	25	23	14	11	18	28	5	22	15	1	24	29	4	10	19	9	16	30	7	2	27	21	12	31	6	8	17	20	13	3	26
0	26	17	11	7	29	22	12	14	20	31	5	9	19	24	2	28	6	13	23	27	1	10	16	18	8	3	25	21	15	4	30
0	27	19	8	3	24	16	11	6	29	21	14	5	30	22	13	12	23	31	4	15	20	28	7	10	17	25	2	9	18	26	1
0	28	29	1	31	3	2	30	27	7	6	26	4	24	25	5	19	15	14	18	12	16	17	13	8	20	21	9	23	11	10	22
0	29	31	2	27	6	4	25	19	14	12	17	8	21	23	10	3	30	28	1	24	5	7	26	16	13	15	18	11	22	20	9
0	30	25	7	23	9	14	16	11	21	18	12	28	2	5	27	22	8	15	17	1	31	24	6	29	3	4	26	10	20	19	13
0	31	27	4	19	12	8	23	3	28	24	7	16	15	11	20	6	25	29	2	21	10	14	17	5	26	30	1	22	9	13	18

Table 10: Multiplication table in the Galois field $\mathbb{F}_{2^5}$ (numeric values).

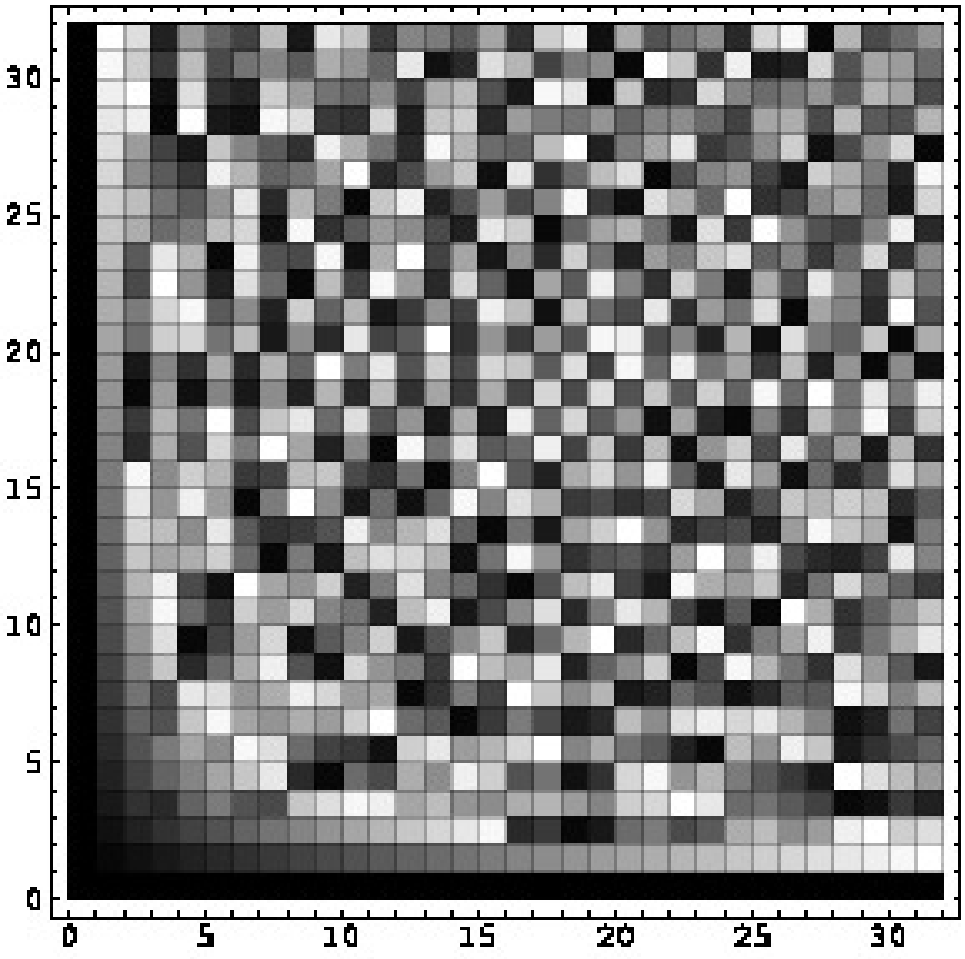
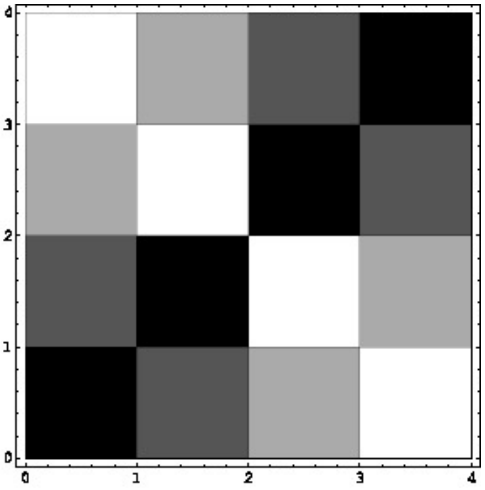


Table 11: Multiplication table in the Galois field $\mathbb{F}_{2^5}$ (density plot).

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

(a)



(b)

Table 12: Addition table in $[\![0, 2^2 - 1]\!]$ corresponding to addition in the Galois field $\mathbb{F}_{2^2}$.

4.2 Addition

What has been done for the multiplication can also be done for the addition in the Galois field $\mathbb{F}_{2^n}$. Indeed, addition is performed as the polynomial addition reduced modulus 2. Using the above identification the field addition determines the operation

$$\oplus : [\![0, 2^n - 1]\!] \times [\![0, 2^n - 1]\!] \to [\![0, 2^n - 1]\!] \ , \ (I_{\boldsymbol{\epsilon}}, I_{\boldsymbol{\delta}}) \mapsto I_{\boldsymbol{\gamma}},$$

where the vector index $\boldsymbol{\gamma}$ is such that $p_{\boldsymbol{\gamma}}(X) = p_{\boldsymbol{\epsilon}}(X) + p_{\boldsymbol{\delta}}(X)$. In tables 12-16 these operations are displayed for $n = 2, 3, 4, 5$ respectively.

5 Field operations with the discrete logarithm representation

5.1 Multiplication

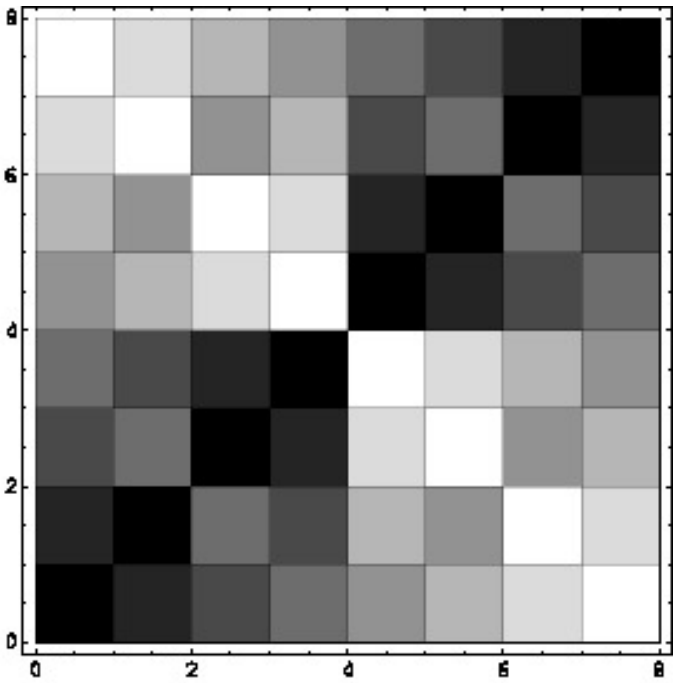
The multiplication group $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} - \{0\}$ of the Galois field $\mathbb{F}_{2^n}$ is cyclic, hence for any primitive element $x_0 \in \mathbb{F}_{2^n}^*$ we have that for all $x \in \mathbb{F}_{2^n}^*$ there is a $y \in [\![0, 2^n - 2]\!]$ such that $x = x_0^y$. Obviously, it is written $y = \log_{x_0}(x)$. Through this function, the multiplication can be expressed additively: $\log_{x_0}(x_1 x_2) = \log_{x_0}(x_1) + \log_{x_0}(x_2)$. Let $J : \mathbb{F}_{2^n} \to [\![0, 2^n - 1]\!]$ be the map such that $J(0) = 0$ and $J(x) = \log_{x_0}(x) + 1$. Hence J is a bijection and the multiplication in $\mathbb{F}_{2^n}$ determines an operation $* : [\![0, 2^n - 1]\!] \times [\![0, 2^n - 1]\!] \to [\![0, 2^n - 1]\!]$, which is the multiplication using the discrete logarithm representation. These operations are displayed in tables 17-21.

5.2 Addition

Also, in terms of a primitive element $x_0 \in \mathbb{F}_{2^n}^*$ we may express the elements of $\mathbb{F}_{2^n}$ through the map $J : \mathbb{F}_{2^n} \to [\![0, 2^n - 1]\!]$ such that $J(0) = 0$ and $J(x) = \log_{x_0}(x) + 1$. For any $i, j \in [\![0, 2^n - 2]\!]$, with $i \leq j$, we have $x_0^i + x_0^j = x_0^i(1 + x_0^{j-i}) = x_0^{i+k}$, where the addition is taken modulus $2^n - 1$ and $x_0^k = (1 + x_0^{j-i})$, or $p_{nk}(X) | \, 1 + x_0^{j-i} + x_0^k$. Thus, addition involves the irreducible polynomial $p_{nk}(X)$. The corresponding form of addition for $n = 2, 3, 4, 5$ are displayed in tables 22-26.

0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	0	1	6	7	4	5
3	2	1	0	7	6	5	4
4	5	6	7	0	1	2	3
5	4	7	6	1	0	3	2
6	7	4	5	2	3	0	1
7	6	5	4	3	2	1	0

(a)

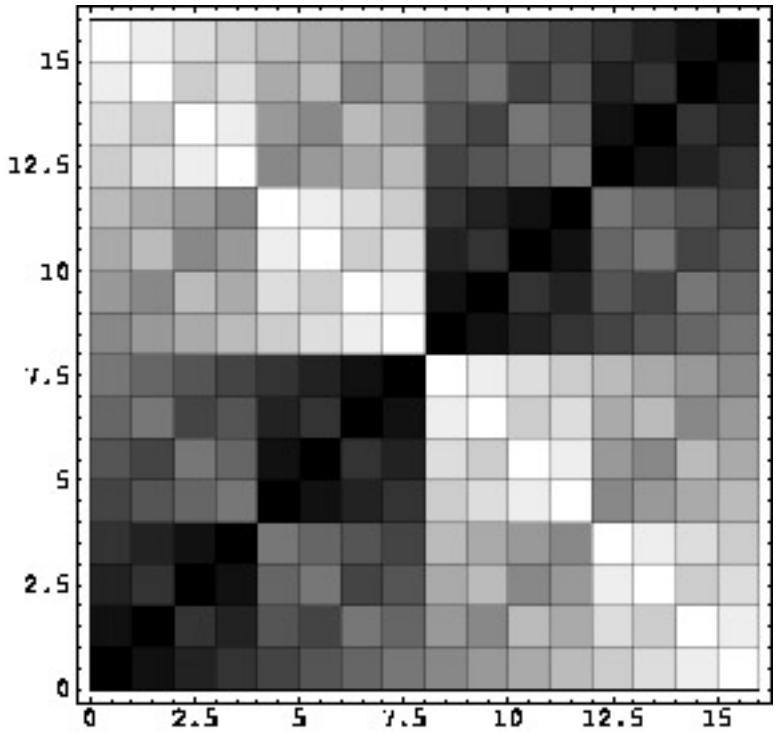


(b)

Table 13: Addition table in $[\![0, 2^3 - 1]\!]$ corresponding to addition in the Galois field $\mathbb{F}_{2^3}$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

(a)



(b)

Table 14: Addition table in $[\![0, 2^4 - 1]\!]$ corresponding to addition in the Galois field $\mathbb{F}_{2^4}$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14	17	16	19	18	21	20	23	22	25	24	27	26	29	28	31	30
2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13	18	19	16	17	22	23	20	21	26	27	24	25	30	31	28	29
3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12	19	18	17	16	23	22	21	20	27	26	25	24	31	30	29	28
4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11	20	21	22	23	16	17	18	19	28	29	30	31	24	25	26	27
5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10	21	20	23	22	17	16	19	18	29	28	31	30	25	24	27	26
6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9	22	23	20	21	18	19	16	17	30	31	28	29	26	27	24	25
7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	23	22	21	20	19	18	17	16	31	30	29	28	27	26	25	24
8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7	24	25	26	27	28	29	30	31	16	17	18	19	20	21	22	23
9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6	25	24	27	26	29	28	31	30	17	16	19	18	21	20	23	22
10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5	26	27	24	25	30	31	28	29	18	19	16	17	22	23	20	21
11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4	27	26	25	24	31	30	29	28	19	18	17	16	23	22	21	20
12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3	28	29	30	31	24	25	26	27	20	21	22	23	16	17	18	19
13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2	29	28	31	30	25	24	27	26	21	20	23	22	17	16	19	18
14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1	30	31	28	29	26	27	24	25	22	23	20	21	18	19	16	17
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	16	19	18	21	20	23	22	25	24	27	26	29	28	31	30	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
18	19	16	17	22	23	20	21	26	27	24	25	30	31	28	29	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
19	18	17	16	23	22	21	20	27	26	25	24	31	30	29	28	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
20	21	22	23	16	17	18	19	28	29	30	31	24	25	26	27	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
21	20	23	22	17	16	19	18	29	28	31	30	25	24	27	26	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
22	23	20	21	18	19	16	17	30	31	28	29	26	27	24	25	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
23	22	21	20	19	18	17	16	31	30	29	28	27	26	25	24	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
24	25	26	27	28	29	30	31	16	17	18	19	20	21	22	23	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
25	24	27	26	29	28	31	30	17	16	19	18	21	20	23	22	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
26	27	24	25	30	31	28	29	18	19	16	17	22	23	20	21	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
27	26	25	24	31	30	29	28	19	18	17	16	23	22	21	20	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
28	29	30	31	24	25	26	27	20	21	22	23	16	17	18	19	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
29	28	31	30	25	24	27	26	21	20	23	22	17	16	19	18	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
30	31	28	29	26	27	24	25	22	23	20	21	18	19	16	17	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Table 15: Addition table in $[\![0, 2^5 - 1]\!]$ corresponding to addition in the Galois field $\mathbb{F}_{2^5}$ (numeric values).

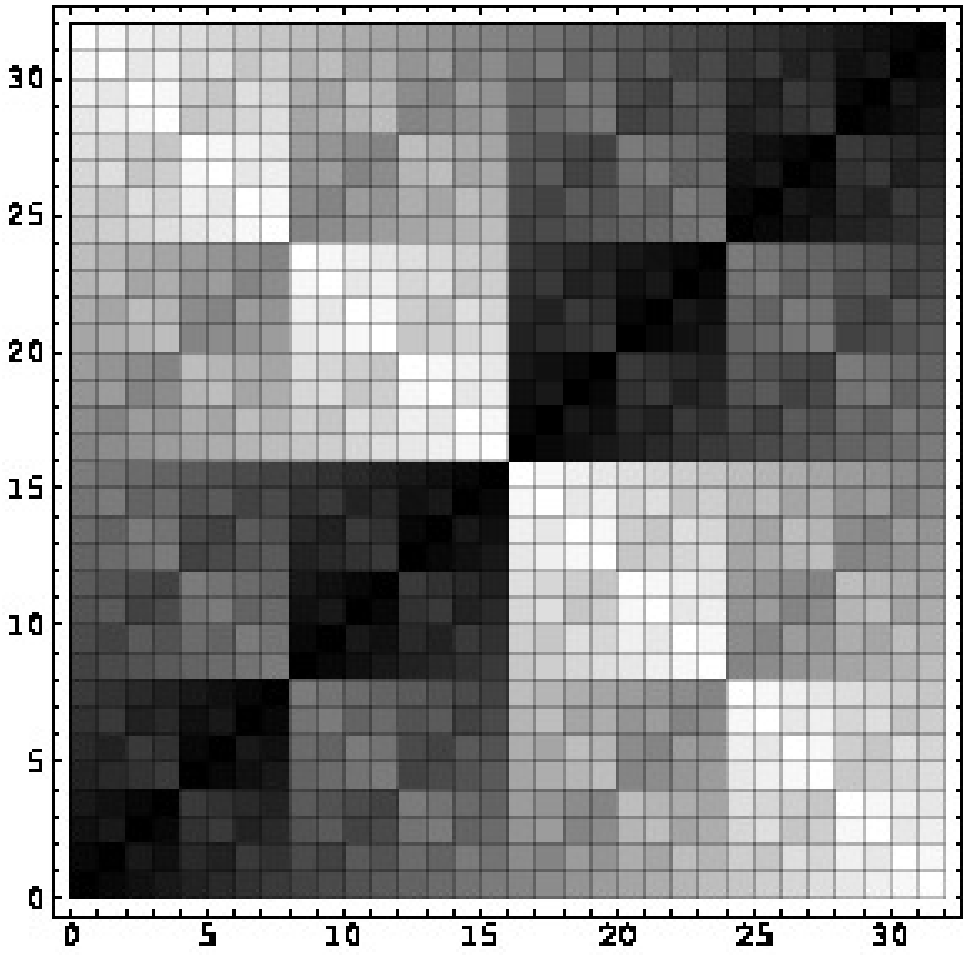
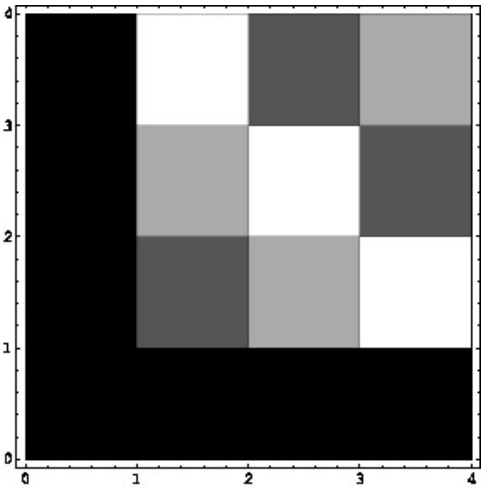


Table 16: Addition table in $[\![0, 2^5 - 1]\!]$ corresponding to addition in the Galois field $\mathbb{F}_{2^5}$ (density plot).

0	0	0	0
0	1	2	3
0	2	3	1
0	3	1	2

(a)

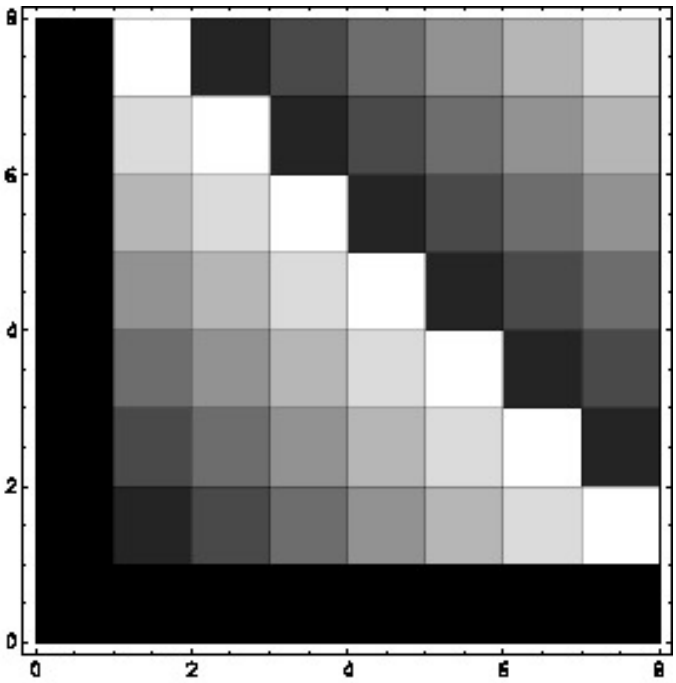


(b)

Table 17: Logarithmic multiplication table in $[\![0, 2^2 - 1]\!]$ using map J.

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	2	3	4	5	6	7	1
0	3	4	5	6	7	1	2
0	4	5	6	7	1	2	3
0	5	6	7	1	2	3	4
0	6	7	1	2	3	4	5
0	7	1	2	3	4	5	6

(a)

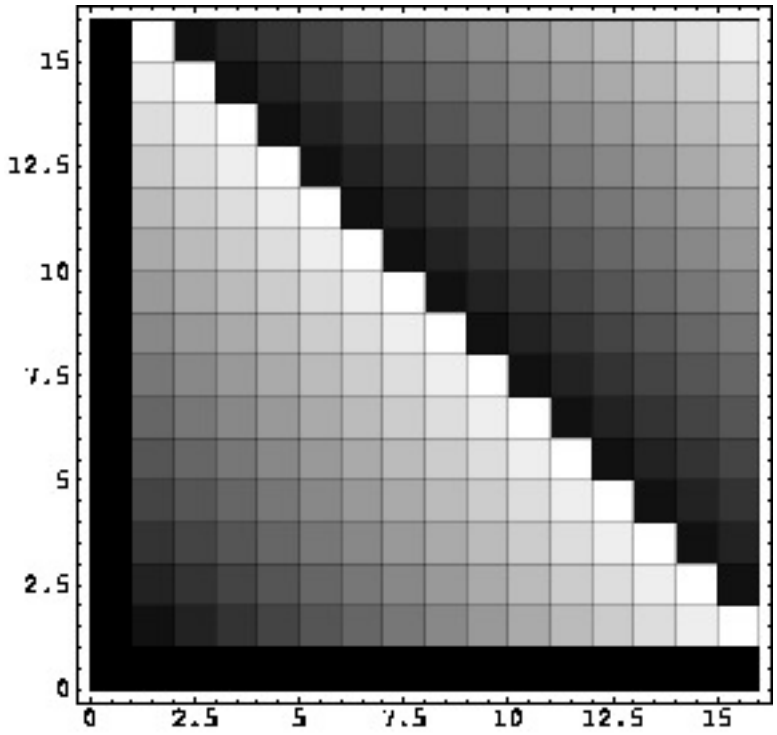


(b)

Table 18: Logarithmic multiplication table in $[\![0, 2^3 - 1]\!]$ using map J.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1
0	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2
0	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3
0	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4
0	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5
0	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
0	8	9	10	11	12	13	14	15	1	2	3	4	5	6	7
0	9	10	11	12	13	14	15	1	2	3	4	5	6	7	8
0	10	11	12	13	14	15	1	2	3	4	5	6	7	8	9
0	11	12	13	14	15	1	2	3	4	5	6	7	8	9	10
0	12	13	14	15	1	2	3	4	5	6	7	8	9	10	11
0	13	14	15	1	2	3	4	5	6	7	8	9	10	11	12
0	14	15	1	2	3	4	5	6	7	8	9	10	11	12	13
0	15	1	2	3	4	5	6	7	8	9	10	11	12	13	14

(a)



(b)

Table 19: Logarithmic multiplication table in $[\![0, 2^4 - 1]\!]$ using map J.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1
0	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2
0	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3
0	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4
0	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5
0	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6
0	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7
0	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8
0	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9
0	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10
0	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11
0	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12
0	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13
0	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
0	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
0	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Table 20: Logarithmic multiplication table in $[\![0, 2^5 - 1]\!]$ using map J (numeric values).

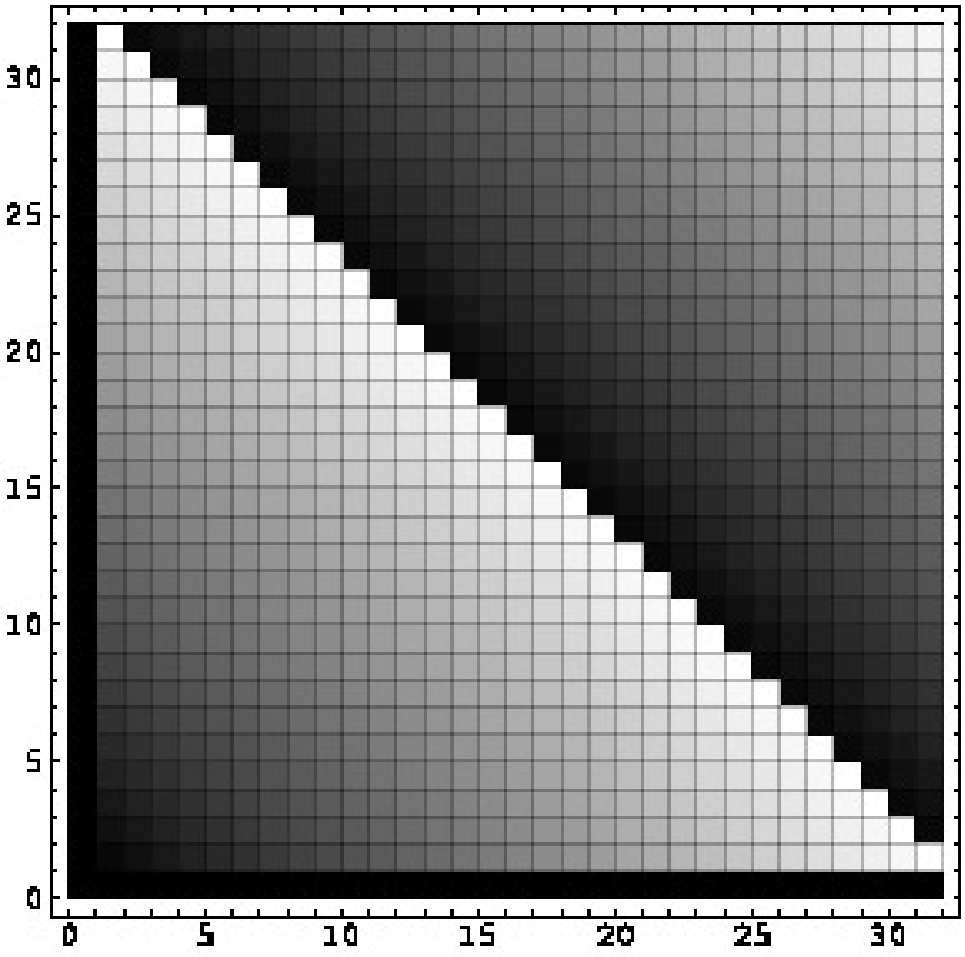
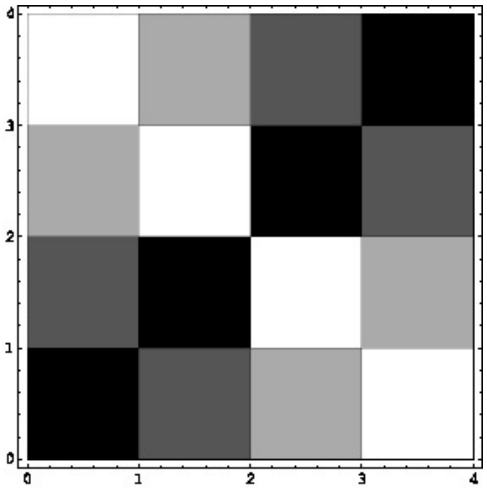


Table 21: Logarithmic multiplication table in $[\![0, 2^5 - 1]\!]$ using map J (density plot).

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

(a)

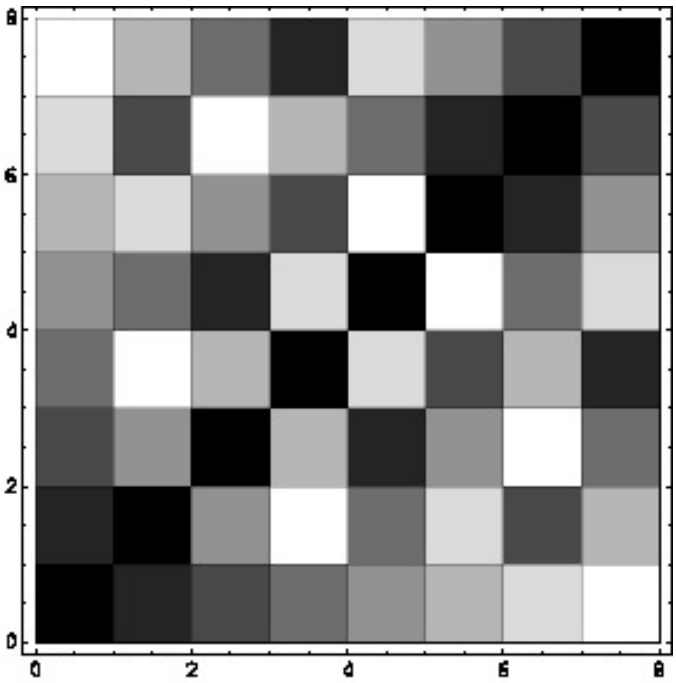


(b)

Table 22: Logarithmic addition table in $[\![0, 2^2 - 1]\!]$ using map J.

0	1	2	3	4	5	6	7
1	0	4	7	3	6	2	5
2	4	0	5	1	4	7	3
3	7	5	0	6	2	5	1
4	3	1	6	0	7	3	6
5	6	4	2	7	0	1	4
6	2	7	5	3	1	0	2
7	5	3	1	6	4	2	0

(a)

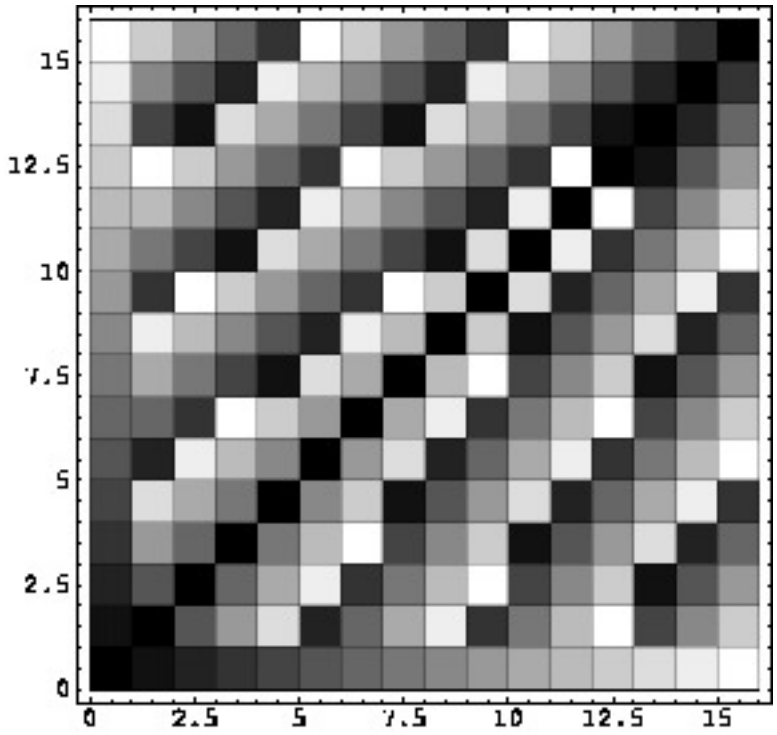


(b)

Table 23: Logarithmic addition table in $[\![0, 2^3 - 1]\!]$ using map J.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	5	9	13	2	6	10	14	3	7	11	15	4	8	12
2	5	0	6	10	14	3	7	11	15	4	8	12	1	5	9
3	9	6	0	7	11	15	4	8	12	1	5	9	13	2	6
4	13	10	7	0	8	12	1	5	9	13	2	6	10	14	3
5	2	14	11	8	0	9	13	2	6	10	14	3	7	11	15
6	6	3	15	12	9	0	10	14	3	7	11	15	4	8	12
7	10	7	4	1	13	10	0	11	15	4	8	12	1	5	9
8	14	11	8	5	2	14	11	0	12	1	5	9	13	2	6
9	3	15	12	9	6	3	15	12	0	13	2	6	10	14	3
10	7	4	1	13	10	7	4	1	13	0	14	3	7	11	15
11	11	8	5	2	14	11	8	5	2	14	0	15	4	8	12
12	15	12	9	6	3	15	12	9	6	3	15	0	1	5	9
13	4	1	13	10	7	4	1	13	10	7	4	1	0	2	6
14	8	5	2	14	11	8	5	2	14	11	8	5	2	0	3
15	12	9	6	3	15	12	9	6	3	15	12	9	6	3	0

(a)



(b)

Table 24: Logarithmic addition table in $[\![0, 2^4 - 1]\!]$ using map J.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14
2	19	0	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28
3	6	20	0	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11
4	24	7	21	0	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25
5	11	25	8	22	0	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8
6	29	12	26	9	23	0	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22
7	16	30	13	27	10	24	0	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5
8	3	17	31	14	28	11	25	0	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19
9	21	4	18	1	15	29	12	26	0	27	14	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2
10	8	22	5	19	2	16	30	13	27	0	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24	11	29	16
11	26	9	23	6	20	3	17	31	14	28	0	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30
12	13	27	10	24	7	21	4	18	1	15	29	0	30	17	4	22	9	27	14	1	19	6	24	11	29	16	3	21	8	26	13
13	31	14	28	11	25	8	22	5	19	2	16	30	0	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27
14	18	1	15	29	12	26	9	23	6	20	3	17	31	0	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10
15	5	19	2	16	30	13	27	10	24	7	21	4	18	1	0	2	20	7	25	12	30	17	4	22	9	27	14	1	19	6	24
16	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	0	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7
17	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	0	4	22	9	27	14	1	19	6	24	11	29	16	3	21
18	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	0	5	23	10	28	15	2	20	7	25	12	30	17	4
19	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	0	6	24	11	29	16	3	21	8	26	13	31	18
20	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	0	7	25	12	30	17	4	22	9	27	14	1
21	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	0	8	26	13	31	18	5	23	10	28	15
22	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	0	9	27	14	1	19	6	24	11	29
23	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	0	10	28	15	2	20	7	25	12
24	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	0	11	29	16	3	21	8	26
25	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	0	12	30	17	4	22	9
26	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	0	13	31	18	5	23
27	4	18	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	0	14	1	19	6
28	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17	31	14	0	15	2	20
29	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	0	16	3
30	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	0	17
31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18	1	15	29	12	26	9	23	6	20	3	17	0

Table 25: Logarithmic addition table in $[\![0, 2^5 - 1]\!]$ using map J (numeric values).

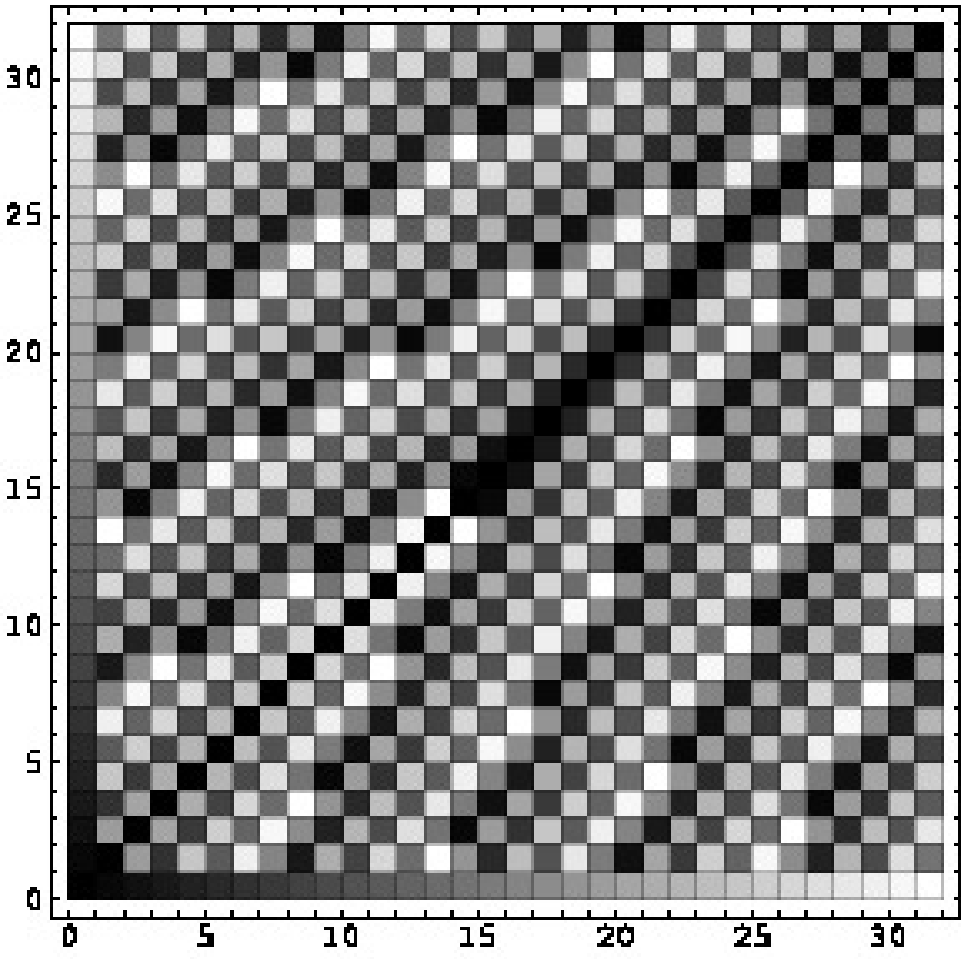


Table 26: Logarithmic addition table in $[\![0, 2^5 - 1]\!]$ using map J (density plot).

6 Algorithms for field arithmetic operations

Let $p_n(X) = X^n + \sum_{j=0}^{n-1} q_j X^j \in \mathbb{F}_2[X]$ be an irreducible polynomial of degree n and let us represent the field $\mathbb{F}_{2^n}$ as $\mathbb{F}_2[X]/(p_n(X))$.

6.1 Multiplication

Let $A(X) = \sum_{i=0}^{n-1} a_i X^i$ and $B(X) = \sum_{j=0}^{n-1} b_j X^j$ be two elements in $\mathbb{F}_{2^n}$ expressed with respect to the polynomial basis. Then

$$A(X)\ B(X) = \left(\sum_{i=0}^{n-1} a_i X^i\right)\ B(X) = \sum_{i=0}^{n-1} a_i \left(X^i\ B(X)\right). \tag{1}$$

Besides,

$$X^{i+1}\ B(X) = X(X^i\ B(X)) \qquad \text{and} \tag{2}$$

$$X\ B(X) = X \sum_{j=0}^{n-1} b_j X^j = b_{n-1}X^n + \sum_{j=1}^{n-1} b_{j-1}X^j = b_{n-1}q_0 + \sum_{j=1}^{n-1} \left[b_{j-1} + b_{n-1}q_j\right] X^j. \tag{3}$$

Clearly, eq's (1)-(3) determine an algorithm to compute the multiplication.

As a second procedure, let us recall the famous *Karatsuba-Ofman*. Let us split the factors as

$$\begin{aligned} A(X) &= \sum_{i=0}^{n-1} a_i X^i = \sum_{i=0}^{\frac{n}{2}-1} a_i X^i + \sum_{i=\frac{n}{2}}^{n-1} a_i X^i = A_\ell(X) + X^{\frac{n}{2}} A_h(X) \\ B(X) &= \sum_{i=0}^{n-1} b_i X^i = \sum_{i=0}^{\frac{n}{2}-1} b_i X^i + \sum_{i=\frac{n}{2}}^{n-1} b_i X^i = B_\ell(X) + X^{\frac{n}{2}} B_h(X) \end{aligned}$$

where $A_\ell(X), A_h(X), B_\ell(X), B_h(X)$ are polynomials of degree $\frac{n}{2} - 1$. Thus

$$\begin{aligned} A(X)\ B(X) &= \left(A_\ell(X) + X^{\frac{n}{2}} A_h(X)\right)\left(B_\ell(X) + X^{\frac{n}{2}} B_h(X)\right) \\ &= A_\ell(X)B_\ell + \left(A_\ell(X)B_h + A_h(X)B_\ell(X)\right)\ X^{\frac{n}{2}} + A_h(X)B_h(X)\ X^{n-1} \\ &= A_\ell(X)B_\ell \\ &\quad + \left[\left(A_\ell(X) + A_h(X)\right)\left(B_\ell(X) + B_h(X)\right) + A_\ell(X)B_\ell + A_h(X)B_h(X)\right]\ X^{\frac{n}{2}} \\ &\quad + A_h B_h(X)\ X^{n-1} \end{aligned} \tag{4}$$

Eq. (4) determines a divide-and-conquer algorithm for multiplication. If n is a power of 2, $n = 2^k$, and $T(n)$ counts the number of $\mathbb{F}_2$-operations to perform the multiplication in $\mathbb{F}_{2^n}$ then the following recursion results from (4):

$$S(k) = T(n) = 3T\left(\frac{n}{2}\right) = 3S(k-1) \quad , \quad S(0) = T(1) = 1,$$

and its solution is $S(k) = 3^k$, namely $T(n) = 3^{\log_2 n} = n^{\log_2 3}$, thus the ratio $\frac{T(n)}{n^2} = n^{-(2-\log_2 n)}$ tends to 0 as $n \nearrow +\infty$.

6.2 Squaring

Since $\mathbb{F}_{2^n}$ is a field of characteristic 2, squaring is a linear map, thus

$$A(X) = \sum_{i=0}^{n-1} a_i X^i \implies A(X)^2 = \sum_{i=0}^{n-1} a_i X^{2i}, \tag{5}$$

thus only monomials of even exponent appear in $A(X)^2$.

If $n = 2k$ is an even number,

$$\begin{aligned} A(X)^2 &= \sum_{i=0}^{k-1} a_i X^{2i} + \sum_{i=k}^{n-1} a_i X^{2i} \\ &= \sum_{i=0}^{k-1} a_i X^{2i} + X^n \sum_{i=0}^{k-1} a_{k+i} X^{2i} \\ &= \sum_{i=0}^{k-1} a_i X^{2i} + \left(\sum_{j=0}^{n-1} q_j X^j \right) \left(\sum_{i=0}^{k-1} a_{k+i} X^{2i} \right) \end{aligned} \tag{6}$$

If $n = 2k - 1$ is an odd number,

$$\begin{aligned} A(X)^2 &= \sum_{i=0}^{k-1} a_i X^{2i} + \sum_{i=k}^{n-1} a_i X^{2i} \\ &= \sum_{i=0}^{k-1} a_i X^{2i} + X^{n+1} \sum_{i=0}^{k-2} a_{k+i} X^{2i} \\ &= \sum_{i=0}^{k-1} a_i X^{2i} + \left(\sum_{j=0}^{n-1} q_j X^j \right) \left(\sum_{i=0}^{k-2} a_{k+i} X^{2i+1} \right) \end{aligned} \tag{7}$$

Eq's (6)-(7) determine an algorithm for squaring, which can still be simplified, according to the special form of the irreducible polynomial $p_n(X)$.

6.3 Square root

Since $\mathbb{F}_{2^n}^*$ is a cyclic group of order $2^n - 1$ we have that for all $A(X) \in \mathbb{F}_{2^n}$: $A(X) = A(X)^{2^n} = \left(A(X)^{2^{n-1}} \right)^2$, thus $\sqrt{A(X)} = A(X)^{2^{n-1}}$, and being squaring a linear map:

$$A(X) = \sum_{i=0}^{n-1} a_i X^i \implies \sqrt{A(X)} = \sum_{i=0}^{n-1} a_i \left(X^{2^{n-1}} \right)^i = \sum_{i=0}^{n-1} a_i \left(\sqrt{X} \right)^i. \tag{8}$$

If $n = 2k$ is an even number,

$$\begin{aligned} \sqrt{A(X)} &= \sum_{i=0}^{k-1} a_{2i} \left(\sqrt{X} \right)^{2i} + \sum_{i=0}^{k-1} a_{2i+1} \left(\sqrt{X} \right)^{2i+1} \\ &= \sum_{i=0}^{k-1} a_{2i} X^i + \sqrt{X} \sum_{i=0}^{k-1} a_{2i+1} X^i \end{aligned} \tag{9}$$

If $n = 2k - 1$ is an odd number,

$$\begin{aligned} \sqrt{A(X)} &= \sum_{i=0}^{k-1} a_{2i} \left(\sqrt{X} \right)^{2i} + \sum_{i=0}^{k-2} a_{2i+1} \left(\sqrt{X} \right)^{2i+1} \\ &= \sum_{i=0}^{k-1} a_{2i} X^i + \sqrt{X} \sum_{i=0}^{k-2} a_{2i+1} X^i \end{aligned} \tag{10}$$

and clearly, $\sqrt{X} = X^{2^{n-1}} \bmod p_n(X)$.

6.4 Trace

If $m|n$ then $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$, or $\mathbb{F}_{2^n}$ is an extension of $\mathbb{F}_{2^m}$. In this case, the map

$$T_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m} \quad x \mapsto \sum_{k=0}^{\frac{n}{m}-1} x^{2^{mk}}$$

is called the *trace*. T_m^n is a $\mathbb{F}_{2^m}$-linear map. Consequently,

$$A(X) = \sum_{i=0}^{\frac{n}{m}-1} a_i X^i \ , \ a_i \in \mathbb{F}_m \implies T_m^n(A(X)) = \sum_{i=0}^{\frac{n}{m}-1} a_i T_m^n(X^i). \tag{11}$$

And,

$$T_m^n(X^i) = \left(\sum_{k=0}^{\frac{n}{m}-1} X^{2^{mk} i} \right) \bmod p_{nm}(X), \tag{12}$$

where $p_{nm}(X) \in \mathbb{F}_m[X]$ is an irreducible polynomial of degree $\frac{n}{m}$. Then by pre-computing the values at (12), the values of the trace can be calculated according to relation (11).

References

[1] Liedl, H., Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.