УДК 004.052.44

ЭФФЕКТИВНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СХЕМЫ ДЛЯ АРИФМЕТИКИ ПОЛЯ ГАЛУА GF(2^8) В ТЕХНОЛОГИИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Рахман П.А.

ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Филиал в г. Стерлитамаке, e-mail: pavelar@yandex.ru

В рамках данной статьи рассматривается арифметика поля Галуа GF(2^8) на базе неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, применяемого в технологии помехоустойчивого кодирования информации. Также рассматривается схема формирования таблиц степеней и логарифмов на базе примитивного элемента $\alpha = 2$, формулы сложения, умножения и деления, а также инвертирования элементов и возведения в заданную степень. Приводятся примеры выполнения арифметических операций с элементами поля. Также рассматриваются высокопроизводительные схемы прямого умножения и инвертирования элементов.

Ключевые слова: поле Галуа, арифметика, эффективные вычисления, помехоустойчивое кодирование информации

EFFECTIVE COMPUTATIONAL SCHEMES FOR THE ARITHMETIC OF GALOIS FIELD GF(2^8) IN THE ERROR-CORRECTING CODING TECHNOLOGY

Rahman P.A.

Ufa State Petroleum Technological University, Sterlitamak branch, e-mail: pavelar@yandex.ru

This paper deals with the arithmetic of Galois Field GF(2^8) based on the irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, which is widely used in error-correcting coding technologies. The schemes for generating the tables of logarithms and anti-logarithms on base of the primitive element $\alpha = 2$, formula for the addition, multiplication, division, inversion of field elements and powering elements to the given degree are also discussed. Calculation examples of arithmetic operations with the field elements are also provided. The high-performance schemes of the direct multiplication and inversion of the field elements are also observed.

Keywords: Galois field, arithmetic, effective computations, error-correcting coding

На сегодняшний день информация играет ключевую роль, как в жизни отдельного человека, так и в бизнес-процессах предприятий. Соответственно, защита ее от искажения в системах хранения и каналах передачи данных при помощи технологии помехоустойчивого кодирования является актуальной задачей [1]. Однако, современные технологии помехоустойчивого кодирования данных [2] базируются на специализированных разделах математики, в частности, арифметике полей Галуа $GF(2^8)$, и для разработки программных или аппаратных реализаций, требуются дополнительные исследования [3-8] и выведение достаточно простых для понимания, и в то же время, высокопроизводительных вычислительных схем для конкретных технологий помехоустойчивого кодирования.

Арифметика поля Галуа $GF(2^8)$ с применением логарифмов в технологии помехоустойчивого кодирования на базе кодов Рида-Соломона. Поле Галуа $GF(2^8)$ является частным случаем расширенных конечных полей $GF(2^m)$ характеристики 2 и имеет широкое применение в технологиях помехоустойчивой передачи и хранения информации благодаря тому, что основной единицей информации в вычислительной технике является байт. Байт состоит 8 битов и с помощью него можно представить 256 различных символов, и поле Галуа $GF(2^8)$ также содержит 256 элементов, которые также можно представить в виде 8-разрядных двоичных чисел.

Яркие примеры использования арифметики поля Галуа $GF(2^8)$: помехоустойчивое кодирование с применением кодов Рида-Соломона для хранения информации на оптических дисках с данными – Data CD-ROM и при передаче информации в стандарте цифрового телевещания DVB – Digital Video Broadcasting.

Поле Галуа $GF(2^8)$ по определению содержит 256 элементов:

	$a(x)$:	0	1	x	…	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$GF(2^8)$:	$(a)_2$:	00000000	00000001	00000010	…	11111111
	$(a)_{10}$:	0	1	2	…	255

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	4	8	16	32	64	128	29	58	116	232	205	135	19	38
16	76	152	45	90	180	117	234	201	143	3	6	12	24	48	96	192
32	157	39	78	156	37	74	148	53	106	212	181	119	238	193	159	35
48	70	140	5	10	20	40	80	160	93	186	105	210	185	111	222	161
64	95	190	97	194	153	47	94	188	101	202	137	15	30	60	120	240
80	253	231	211	187	107	214	177	127	254	225	223	163	91	182	113	226
96	217	175	67	134	17	34	68	136	13	26	52	104	208	189	103	206
112	129	31	62	124	248	237	199	147	59	118	236	197	151	51	102	204
128	133	23	46	92	184	109	218	169	79	158	33	66	132	21	42	84
144	168	77	154	41	82	164	85	170	73	146	57	114	228	213	183	115
160	230	209	191	99	198	145	63	126	252	229	215	179	123	246	241	255
176	227	219	171	75	150	49	98	196	149	55	110	220	165	87	174	65
192	130	25	50	100	200	141	7	14	28	56	112	224	221	167	83	166
208	81	162	89	178	121	242	249	239	195	155	43	86	172	69	138	9
224	18	36	72	144	61	122	244	245	247	243	251	235	203	139	11	22
240	44	88	176	125	250	233	207	131	27	54	108	216	173	71	142	1

Рис. 1. Таблица степеней 2^k для поля Галуа $GF(2^8)$

Поле Галуа $GF(2^8)$, по определению являющееся полем многочленов вида $a(x) = a_7x^7 + \ldots + a_1x + a_0$, образуется на базе простого поля Галуа $GF(2)$ и неприводимого многочлена 8-й степени. В технологии помехоустойчивого кодирования используется неприводимый многочлен следующего вида:

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1. \qquad (1)$$

В двоичном представлении неприводимый многочлен выглядит как: $(p)_2 = 100011101$, а в десятичном представлении: $(p)_{10} = 285$.

В качестве примитивного элемента поля $GF(2^8)$ в технологии помехоустойчивого кодирования выбирают элемент $\alpha(x) = x$. При помощи него можно получить все ненулевые элементы поля. В двоичном представлении примитивный элемент поля выглядит как $(\alpha)_2 = 10$, а в десятичном представлении, соответственно, как $(\alpha)_{10} = 2$.

Для формирования таблицы степеней примитивного элемента $(\alpha)_{10} = 2$ используется представленная ниже рекуррентная схема для случая поля Галуа $GF(2^8)$ с неприводимым многочленом $p(x) = x^8 + x^4 + x^3 + x + 1$. Что касается таблицы логарифмов, то ее можно формировать параллельно с формированием таблицы степеней, используя десятичное представление степеней примитивного элемента в качестве индексов таблицы логарифмов.

$$\begin{cases} k = 1 \ldots 2^8 - 2; \quad \alpha^0 = 1; \quad \log_\alpha(\alpha^0) = 0; \\ \alpha^k = \begin{cases} \alpha^{k-1} << 1, \quad \alpha_7^{(k-1)} = 0; \\ (\alpha^{k-1} << 1) \oplus (100011101)_2, \quad \alpha_7^{(k-1)} = 1; \end{cases} \\ \log_\alpha(\alpha^k) = k. \end{cases} \qquad (2)$$

Под выражением $\alpha^{k-1} << 1$ понимается сдвиг двоичного числа влево на один разряд. Под выражением $(\alpha^{k-1} << 1) \oplus (100011101)_2$ понимается сдвиг двоичного числа влево на один разряд с последующей операцией «побитового» XOR результата сдвига с двоичным эквивалентом примитивного неприводимого многочлена.

Примечание. Поскольку в десятичном виде примитивный элемент поля $GF(2^8)$ выглядит как $(\alpha)_{10} = 2$, то будем также обозначать k-ую степень примитивного элемента как 2^k, а логарифм от элемента a по основанию примитивного элемента как $\log_2 a$.

Ниже на рис. 1 (в виде матрицы 16 х 16) приведены степени примитивного элемента $(\alpha)_{10} = 2$ поля $GF(2^8)$, образованного при помощи примитивного неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. Степени примитивного элемента для компактности приведены в десятичном представлении, и расположены построчно (по 16 в строке), начиная с 0-й степени, и заканчивая 255-й. Заметим, что 255-я степень эквивалентна 0-й степени и равна 1 в силу свойств конечных полей Галуа $GF(p^m)$: $\alpha^{(p^m - 1)} = \alpha^0 \Rightarrow \alpha^{(2^8 - 1)} = \alpha^0$.

Примечание 1. Для того, чтобы выбрать в таблице требуемую степень 2^k, необходимо выбрать строку и столбец таким образом, чтобы сумма индексов строки и столбца (индексы строк приведены в левом заголовочном столбце серого цвета, индексы столбцов – в верхней заголовочной строке серого цвета) была равна показателю степени k.

Также ниже на рис. 2 (в виде матрицы 16 х 16) приведены логарифмы по основанию примитивного элемента $(\alpha)_{10} = 2$ поля $GF(2^8)$. Логарифмы расположены построчно (по 16 в строке) для всех элементов поля, начиная с $(a)_{10} = 0$, заканчивая $(a)_{10} = 255$. Заметим, что логарифм от 0 не существует (соответствующая ячейка «N/A»).

Примечание 2. Для того, чтобы выбрать в таблице логарифм $\log_2 a$ заданного элемента a поля $GF(2^8)$, необходимо выбрать строку и столбец таким образом, чтобы сумма индексов строки и столбца (индексы строк приведены в левом заголовочном столбце серого цвета, индексы столбцов – в верхней заголовочной строке серого цвета) была равна десятичному представлению (эквиваленту) элемента a.

Тогда с учетом всего вышесказанного имеем арифметику поля Галуа $GF(2^8)$, образованного с помощью неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x^2 + 1$ и на базе применения логарифмов по основанию примитивного элемента $(\alpha)_{10} = 2$:

$$\underbrace{a \pm b}_{GF(2^8)} = ((a_7 \oplus b_7)\ldots(a_0 \oplus b_0))_2 = a \oplus b.$$

- $GF(2^8)$

$$\underbrace{a \cdot b}_{GF(2^8)} = \begin{cases} \overbrace{2^{(\log_2 a + \log_2 b) \bmod (2^8 - 1)}}^{< R, \{+, \cdot\} >} & a \neq 0 \,\&\, b \neq 0; \\ 0 & a = 0 \vee b = 0. \end{cases} \quad (3)$$

$$\underbrace{a / b}_{GF(2^8)} = \begin{cases} \overbrace{2^{(\log_2 a + ((2^8 - 1) - \log_2 b)) \bmod (2^8 - 1)}}^{< R, \{+, \cdot\} >} & a \neq 0 \,\&\, b \neq 0; \\ 0 & a = 0 \,\&\, b \neq 0; \\ \textit{Ошибка} & b = 0. \end{cases}$$

Кроме того, если необходимо найти обратный элемент по умножению, то можно воспользоваться упрощенным вариантом формулы деления элементов:

$$\underbrace{a^{-1}}_{GF(2^8)} = \begin{cases} \overbrace{2^{((2^8 - 1) - \log_2 a) \bmod (2^8 - 1)}}^{< R, \{+, \cdot\} >} & a \neq 0; \\ \textit{Ошибка} & a = 0. \end{cases} \quad (4)$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	N/A	0	1	25	2	50	26	198	3	223	51	238	27	104	199	75
16	4	100	224	14	52	141	239	129	28	193	105	248	200	8	76	113
32	5	138	101	47	225	36	15	33	53	147	142	218	240	18	130	69
48	29	181	194	125	106	39	249	185	201	154	9	120	77	228	114	166
64	6	191	139	98	102	221	48	253	226	152	37	179	16	145	34	136
80	54	208	148	206	143	150	219	189	241	210	19	92	131	56	70	64
96	30	66	182	163	195	72	126	110	107	58	40	84	250	133	186	61
112	202	94	155	159	10	21	121	43	78	212	229	172	115	243	167	87
128	7	112	192	247	140	128	99	13	103	74	222	237	49	197	254	24
144	227	165	153	119	38	184	180	124	17	68	146	217	35	32	137	46
160	55	63	209	91	149	188	207	205	144	135	151	178	220	252	190	97
176	242	86	211	171	20	42	93	158	132	60	57	83	71	109	65	162
192	31	45	67	216	183	123	164	118	196	23	73	236	127	12	111	246
208	108	161	59	82	41	157	85	170	251	96	134	177	187	204	62	90
224	203	89	95	176	156	169	160	81	11	245	22	235	122	117	44	215
240	79	174	213	233	230	231	173	232	116	214	244	234	168	80	88	175

Рис. 2. Таблица логарифмов $\log_2 a$ для поля Галуа $GF(2^8)$

Наконец, для возведения в степень v заданного элемента a поля $GF(2^8)$ можно использовать формулу, применив операцию модулярного умножения логарифмов:

$$\bullet \quad \overbrace{a^{v}}^{GF(2^8)} = \begin{cases} 2^{\overbrace{(v\log_2 a)\bmod(2^8-1)}^{<R,\{+,\cdot\}>}} & a \neq 0 \,\&\, v \geq 0; \\ 0 & a = 0 \,\&\, v > 0; \\ 1 & a = 0 \,\&\, v = 0. \end{cases} \tag{5}$$

Пример 1. Найдем сумму элементов расширенного поля $GF(2^8)$, представленных в виде соответствующих чисел «123» и «231» в десятичной системе счисления. Имеем,

$$\underbrace{(123)_{10} + (231)_{10}}_{GF(2^8)} = \underbrace{(01111011)_2 + (11100111)_2}_{GF(2^8)} = \left\{ \begin{array}{c|c|c|c|c|c|c|c} \overset{0}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} & \overset{0}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{array} \right\} =$$

$$= (10011100)_2 = (156)_{10}.$$

Таким образом, $\underbrace{(123)_{10} + (231)_{10}}_{GF(2^8)} = (156)_{10}$.

Пример 2. Найдем произведение элементов поля $GF(2^8)$, представленных в виде соответствующих чисел «20» и «11» в десятичной системе счисления. По таблице логарифмов для поля $GF(2^8)$ имеем логарифмы элементов: $\log_2(20)_{10} = 52$ и $\log_2(11)_{10} = 238$. Тогда получаем:

$$\overbrace{(20)_{10} \cdot (11)_{10}}^{GF(2^8)} = 2^{\overbrace{(52+238)\bmod(255)}^{<R,\{+,\cdot\}>}} = 2^{35}.$$

По таблице степеней для поля $GF(2^8)$ имеем $2^{35} = (156)_{10}$. Таким образом:

$$\overbrace{(20)_{10} \cdot (11)_{10}}^{GF(2^8)} = (156)_{10}$$

Пример 3. Найдем отношение элементов поля $GF(2^8)$, представленных в виде соответствующих чисел «220» и «127» в десятичной системе счисления. По таблице логарифмов для поля $GF(2^8)$ имеем логарифмы элементов: $\log_2(220)_{10} = 187$ и $\log_2(127)_{10} = 87$. Тогда получаем:

$$\overbrace{(220)_{10} / (127)_{10}}^{GF(2^8)} =$$

$$= 2^{\overbrace{(187+(255-87))\bmod(255)}^{<R,\{+,\cdot\}>}} = 2^{100}.$$

По таблице степеней имеем $2^{100} = (17)_{10}$.

Таким образом: $\overbrace{(220)_{10} / (127)_{10}}^{GF(2^8)} = (17)_{10}$.

Пример 4. Найдем обратный элемент по умножению для элемента «111», представленного в десятичном виде. По таблице логарифмов имеем логарифм элемента: $\log_2(111)_{10} = 61$. Тогда обратный элемент:

$$\overbrace{((111)_{10})^{-1}}^{GF(2^8)} = 2^{\overbrace{(255-61)\bmod(255)}^{<R,\{+,\cdot\}>}} = 2^{194}.$$

По таблице степеней имеем $2^{194} = (50)_{10}$.

Таким образом: $\overbrace{((111)_{10})^{-1}}^{GF(2^8)} = (50)_{10}$.

Пример 5. Возведем элемент «13», представленный в десятичном виде, в заданную степень $v = 17$. По таблице логарифмов для поля $GF(2^8)$ имеем логарифм элемента: $\log_2(13)_{10} = 104$. Тогда по формуле получаем:

$$\overbrace{((13)_{10})^{17}}^{GF(2^8)} = 2^{\overbrace{(17\cdot 104)\bmod(255)}^{<R,\{+,\cdot\}>}} = 2^{238}.$$

По таблице степеней имеем $2^{238} = (11)_{10}$.

Таким образом, $\overbrace{((13)_{10})^{17}}^{GF(2^8)} = (11)_{10}$.

Схемы прямого умножения и инвертирования элементов поля Галуа $GF(2^8)$ в технологии помехоустойчивого кодирования информации. В случае необходимости высокопроизводительного прямого умножения элементов a и b поля Галуа $GF(2^8)$, можно использовать заранее подготовленную свертку соответствующих многочленов $a(x)$ и $b(x)$ по модулю неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x^2 + 1$:

$$\underbrace{a \cdot b}_{GF(2^8)} = \underbrace{(a(x) \cdot b(x)) \bmod p(x)}_{GF(2)} = c_7 x^7 + c_6 x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0;$$

$$\begin{cases}
c_0 = a_0 \cdot b_0 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_6 \oplus a_3 \cdot b_5 \oplus a_4 \cdot b_4 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_1 \\
\quad \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_6 \oplus a_7 \cdot b_7; \\
c_1 = a_0 \cdot b_1 \oplus a_1 \cdot b_0 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_6 \oplus a_4 \cdot b_5 \oplus a_5 \cdot b_4 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_6 \oplus a_7 \cdot b_7; \\
c_2 = a_0 \cdot b_2 \oplus a_1 \cdot b_1 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_0 \oplus a_2 \cdot b_6 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_4 \oplus a_4 \cdot b_6 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_5 \\
\quad \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_6; \\
c_3 = a_0 \cdot b_3 \oplus a_1 \cdot b_2 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_1 \oplus a_2 \cdot b_6 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_0 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_6 \oplus a_4 \cdot b_4 \oplus a_4 \cdot b_5 \\
\quad \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_6 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_5 \oplus a_6 \cdot b_6 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_2 \\
\quad \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_5; \\
c_4 = a_0 \cdot b_4 \oplus a_1 \cdot b_3 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_2 \oplus a_2 \cdot b_6 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_1 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_6 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_0 \\
\quad \oplus a_4 \cdot b_4 \oplus a_4 \cdot b_5 \oplus a_4 \cdot b_6 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_5 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_4 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_2 \\
\quad \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_7; \\
c_5 = a_0 \cdot b_5 \oplus a_1 \cdot b_4 \oplus a_2 \cdot b_3 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_2 \oplus a_3 \cdot b_6 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_1 \oplus a_4 \cdot b_5 \oplus a_4 \cdot b_6 \oplus a_4 \cdot b_7 \\
\quad \oplus a_5 \cdot b_0 \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_5 \oplus a_5 \cdot b_6 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_5 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_4; \\
c_6 = a_0 \cdot b_6 \oplus a_1 \cdot b_5 \oplus a_2 \cdot b_4 \oplus a_3 \cdot b_3 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_2 \oplus a_4 \cdot b_6 \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_1 \oplus a_5 \cdot b_5 \oplus a_5 \cdot b_6 \\
\quad \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_0 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_5 \oplus a_6 \cdot b_6 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_5; \\
c_7 = a_0 \cdot b_7 \oplus a_1 \cdot b_6 \oplus a_2 \cdot b_5 \oplus a_3 \cdot b_4 \oplus a_4 \cdot b_3 \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_2 \oplus a_5 \cdot b_6 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_1 \oplus a_6 \cdot b_5 \\
\quad \oplus a_6 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_0 \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_6.
\end{cases}$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	N/A	1	142	244	71	167	122	186	173	157	221	152	61	170	93	150
16	216	114	192	88	224	62	76	102	144	222	85	128	160	131	75	42
32	108	237	57	81	96	86	44	138	112	208	31	74	38	139	51	110
48	72	137	111	46	164	195	64	94	80	34	207	169	171	12	21	225
64	54	95	248	213	146	78	166	4	48	136	43	30	22	103	69	147
80	56	35	104	140	129	26	37	97	19	193	203	99	151	14	55	65
96	36	87	202	91	185	196	23	77	82	141	239	179	32	236	47	50
112	40	209	17	217	233	251	218	121	219	119	6	187	132	205	254	252
128	27	84	161	29	124	204	228	176	73	49	39	45	83	105	2	245
144	24	223	68	79	155	188	15	92	11	220	189	148	172	9	199	162
160	28	130	159	198	52	194	70	5	206	59	13	60	156	8	190	183
176	135	229	238	107	235	242	191	175	197	100	7	123	149	154	174	182
192	18	89	165	53	101	184	163	158	210	247	98	90	133	125	168	58
208	41	113	200	246	249	67	215	214	16	115	118	120	153	10	25	145
224	20	63	230	240	134	177	226	241	250	116	243	180	109	33	178	106
240	227	231	181	234	3	143	211	201	66	212	232	117	127	255	126	253

Рис. 3. Таблица обратных элементов по умножению для поля Галуа GF(2^8)

Аппаратную реализацию схемы умножения мы не будем приводить в силу ее громоздкости. Отметим лишь, что ее несложно построить при помощи 64 двухвходовых логических элементов «И» и 8 многовходовых сумматоров по модулю 2.

Также в случае необходимости применения высокопроизводительного вычислителя обратного элемента по умножению (для ускорения операции деления), можно использовать заранее вычисленную таблицу обратных элементов по умножению.

Ниже на рис. 3 (в виде матрицы 16 х 16) приведены обратные элементы по умножению для элементов поля Галуа $GF(2^8)$, представленные в десятичном виде. Обратные элементы по умножению расположены построчно (по 16 в строке) для всех эле-

ментов поля, начиная с $(a)_{10} = 0$, заканчивая $(a)_{10} = 255$. Заметим, что обратного элемента по умножению для нуля не существует (соответствующая ячейка «N/A»).

Для аппаратной реализации таблицы можно использовать ПЗУ емкостью 256 х 8 бит.

Заключение

Таким образом, в рамках данной статьи рассмотрено поле Галуа $GF(2^8)$ на базе неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, которое применяется в технологии помехоустойчивого кодирования информации. Также рассмотрены схема формирования таблиц степеней и логарифмов на базе примитивного элемента $(\alpha)_{10} = 2$, формулы сложения, умножения и деления, а также инвертирования элементов и возведения в заданную степень. Приведены примеры выполнения арифметических операций с элементами поля. Также рассмотрены высокопроизводительные схемы прямого умножения и инвертирования элементов поля.

Полученные результаты могут быть использованы при разработке эффективных программных и аппаратных реализаций вычислительных блоков в рамках кодирования и декодирования информации с применением кодов Рида-Соломона.

Список литературы

1. Todd K. Moon. Error correcting coding: mathematical methods and algorithms. Hoboken, New Jersey: John Wiley & Sons Inc., 2005.

2. C.K.P Clarke. Reed-Solomon error correction. White Paper WHP 031. British Broadcasting Corporation Research and Development, 2002.

3. Рахман П.А., Григорьева Т.В. Кодирование информации с применением кодов Рида-Соломона. – Уфа: Изд-во УГНТУ, 2015.

4. Рахман П.А. Алгоритм выбора кратности исправляемых искажений для кодирования информации с применением кодов Рида-Соломона // Международный журнал прикладных и фундаментальных исследований, 2015. – № 10-2. – С. 208–212.

5. Рахман П.А. Рекуррентный алгоритм вычисления формальной производной полинома над полем Галуа и его аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-1. – С. 14–18.

6. Рахман П.А. Рекуррентный алгоритм вычисления усеченной свертки полиномов над полем Галуа и его аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-2. – С. 231–235.

7. Рахман П.А. Арифметика поля Галуа на базе схемы сложения и вычитания логарифмов и ее аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-3. – С. 397–402.

8. Рахман П.А. Арифметика поля Галуа на базе быстрого умножения и инвертирования элементов поля и ее аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-3. – С. 403–408.