1 INTRODUÇÃO À ÁLGEBRA EM CAMPOS DE GALOIS $GF(2^m)$

1.1. INTRODUÇÃO

O propósito deste texto é apresentar a conceituação básica da álgebra em Campos de Galois. A abordagem usada para a apresentação deste assunto é descritiva e com vários exemplos com o objetivo de facilitar o entendimento da estrutura algébrica de códigos de bloco lineares, principalmente os BCH (Bose, Chaudhuri e Hocquenghen) e Reed-Solomom (RS), sem nenhum compromisso com o rigor matemático de teoremas e suas respectivas provas.

1.2. CAMPOS

Seja F um conjunto de elementos sobre o qual duas operações binárias, a adição "+" e a multiplicação "•", são definidas. *F,* junto com as duas operações binárias, é um campo se as seguintes condições são satisfeitas:

1. F é um grupo comutativo sob +. O elemento identidade é o 0 (zero).
2. O conjunto dos elementos não zero em F é um grupo comutativo sob •. O elemento identidade é o 1 (um).
3. A multiplicação é distributiva sob adição, i.e., para quaisquer a, b e c em F,

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

A partir da definição pode-se afirmar que um campo possui pelo menos dois elementos: o elemento identidade aditivo e o elemento identidades multiplicativo.

Outras definições preliminares sobre um campo são:

- *Ordem* do campo: é número de elementos que compõem o campo.
- *Elemento aditivo inverso* de a: é representado por $-a$.
- *Elemento multiplicativo inverso* de a: é representado por a^{-1} (dado que $a \neq 0$).
- *Subtração* em um campo: a subtração de um elemento a por outro elemento b, ambos pertencentes a um campo, é definida como

$$a - b \stackrel{\Delta}{=} a + (-b)$$

- *Divisão* em um campo: a divisão de um elemento a por um elemento não zero b, ambos pertencentes a um campo, é definida como

$$a \div b \stackrel{\Delta}{=} a \cdot b^{-1}$$

- *Campos de Galois*: é um campo com um número finito de elementos representado por $GF(p)$, onde p é um número primo.

A partir da definição de um campo, um número básico de propriedades pode ser deduzido. Essas propriedades são:

- Propriedade 1: Para qualquer a $\quad a \cdot 0 = 0 \cdot a$
- Propriedade 2: Para quaisquer a e b não zeros $\quad a \cdot b \neq 0$
- Propriedade 3: Se $\quad a \cdot b = 0 \quad e \quad a \neq 0 \quad \Rightarrow \quad b = 0$
- Propriedade 4: Para quaisquer a e b em um campo $\quad -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$
- Propriedade 5: Para $\quad a \neq 0, \quad a \cdot b = a \cdot c \quad \Rightarrow \quad b = c$

EXEMPLO 1

Considere o conjunto {0, 1} cujas operações de adição e multiplicação módulo-2 são apresentadas nas tabelas a seguir.

+	**0**	**1**
0	0	1
1	1	0

•	**0**	**1**
0	0	0
1	0	1

Este conjunto é um campo de dois elementos sob adição e multiplicação módulo-2, ou seja, é um Campo de Galois, $GF(2) = \{0, 1\}$

* * *

EXEMPLO 2

Seja p um primo. Então, $\{0, 1, 2, \ldots, p - 1\}$ é um conjunto de elementos sob adição módulo-p.Os elementos não zero $\{1, 2, \ldots, p - 1\}$ formam um conjunto comutativo sob multiplicação módulo-p. A partir das definições de adição e multiplicação módulo-p e do fato de que a multiplicação de um número real é distributiva sobre a adição, então a multiplicação módulo-p é distributiva sobre a adição módulo-p. Portanto, o conjunto $\{0, 1, 2, \ldots, p - 1\}$ é um campo de ordem p sob adição e multiplicação módulo-p. Este campo é chamado de campo primo e é representado por $GF(p)$.

Para $p = 2$ tem-se o campo binário apresentado no Exemplo 1. Para $p = 7$, tem-se $GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$ e as operações de adição e multiplicação no campo são:

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

•	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

A subtração e a divisão em $GF(7)$ podem ser resumidas conforme as seguintes operações

$$3-6=3+(-6)=3+1=4$$
$$3\div 2=3\cdot(2^{-1})=3\cdot 4=5$$

* * *

Para qualquer inteiro m é possível estender um campo primo $GF(p)$ com p elementos para um campo estendido $GF(p^m)$ com p^m elementos. A ordem de qualquer campo finito estendido é potência de um primo.

A maioria das regras da aritmética ordinária é aplicada à aritmética dos campos finitos. Mas, como o campo é fechado sob a adição e é finito, deve existir dois inteiros positivos m e n tal que $m < n$, e

$$\sum_{i=1}^{m}1=\sum_{i=1}^{n}1$$

Isso implica que

$$\sum_{i=1}^{n-m}1=0 \quad \Rightarrow \quad \sum_{i=1}^{\lambda}1=0$$

onde λ é o menor positivo inteiro que satisfaz a igualdade e é chamado de *característica* do campo $GF(q)$. A característica λ de um campo finito é primo. Consequentemente, para dois inteiros k e m menores do que λ,

$$\sum_{i=1}^{k}1\neq\sum_{i=1}^{m}1$$

pois

$$\sum_{i=1}^{1}1=1 \quad \sum_{i=1}^{2}1=2 \quad \sum_{i=1}^{3}1=3 \quad \cdots \quad \sum_{i=1}^{\lambda-1}1=\lambda-1 \quad \sum_{i=1}^{\lambda}1=0\,.$$

Portanto existem λ elementos distintos em $GF(q)$. Isso mostra que existe um campo $GF(\lambda)$ sob adição e multiplicação de $GF(q)$, ou seja, $GF(\lambda)$ é um *subcampo* de $GF(q)$ Qualquer campo finito $GF(q)$ com característica λ, contém um subcampo $GF(\lambda)$. Se $q \neq \lambda$, então q é uma potência de λ.

Considere agora a um elemento não zero em $GF(q)$. Deve existir dois inteiros positivos k e m tal que $m > k$ e

$$a^k = a^m$$

multiplicando ambos os lados da equação por a^{-k}, obtém-se

$$1 = a^{m-k}$$

o que implica que deve existir um inteiro n tal que $a^n = 1$. Este valor de n é chamado de *ordem* do elemento a campo $GF(q)$. A sequência $a^1, a^2, a^3, \ldots$ se repete após $a^n = 1$, e suas potências são todas distintas. De fato, tais potências formam um grupo comutativo sob multiplicação em $GF(q)$. Um grupo é dito ser *cíclico* se existir um elemento no grupo cujas potências constituem todo o grupo.

Outras características importantes de um campo finito são:

- Seja a um elemento não zero de um campo finito $GF(q)$. Então

$$a^{q-1} = 1 .$$

- Seja a um elemento não zero de um campo finito $GF(q)$. Seja n a ordem de a. Então n divide q - 1. Em um campo $GF(q)$, um elemento não zero a é dito ser *primitivo* se a ordem de a é q -1.

As potências de um elemento primitivo geram todos os elementos não zero de $GF(q)$. Todo campo finito possui um elemento primitivo

EXEMPLO 3

Considere o $GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$

A característica deste campo é 7. Usando a tabela de multiplicação apresentada no Exemplo 2 as potências de 3 são: $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$. Portanto, a ordem de 3 é 6 e 3 é o elemento primitivo de $GF(7)$. As potências de 4 em $GF(7)$ são: $4^1 = 4$, $4^2 = 2$, $4^3 = 1$. A ordem de 4 é 3, que é um fator de 6.

1.3. ARITMÉTICA NOS CAMPOS BINÁRIOS

Códigos podem ser construídos com símbolos a partir de qualquer campo de Galois $GF(q)$, onde q é um primo p ou uma potência de p. Em geral são construídos a partir de $GF(2)$ ou $GF(2^m)$ e, consequentemente a aritmética usada é a binária. Na aritmética binária a subtração é igual a adição.

A solução de um sistema de equações binárias pode, por exemplo, ser resolvido da forma trivial conforme mostrado a seguir.

$$\begin{aligned} X + Y &= 1 \quad (1) \\ X + Z &= 0 \quad (2) \\ X + Y + Z &= 1 \quad (3) \end{aligned}$$

Somando (1) e (3), obtém-se

$$X + Y + X + Y + Z = 1 + 1 \quad \Rightarrow \quad Z = 0$$

Substituindo $Z = 0$ em (2), obtém-se

$$X + 0 = 0 \quad \Rightarrow \quad X = 0$$

Substituindo $X = 0$ em (1), obtém-se

$$0 + Y = 1 \quad \Rightarrow \quad Y = 1$$

Outra solução usando determinante de terceira ordem seria:

$$\begin{aligned} a_{11}X + a_{12}Y + a_{13}Z &= b_1 \\ a_{21}X + a_{22}Y + a_{23}Z &= b_2 \quad (4) \\ a_{31}X + a_{32}Y + a_{33}Z &= b_3 \end{aligned}$$

Substituindo (1), (2), e (3) em (4), obtém-se

$$\begin{aligned} 1 \cdot X + 1 \cdot Y + 0 \cdot Z &= 1 \\ 1 \cdot X + 0 \cdot Y + 1 \cdot Z &= 0 \quad (5) \\ 1 \cdot X + 1 \cdot Y + 1 \cdot Z &= 1 \end{aligned}$$

A solução para o determinante de terceira ordem é

$$D = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \cdot \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \cdot \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \qquad (6)$$

$$D = a_{11} \cdot (a_{22} \cdot a_{33} - a_{23} \cdot a_{32}) - a_{21} \cdot (a_{12} \cdot a_{33} - a_{13} \cdot a_{32}) + a_{31} \cdot (a_{12} \cdot a_{13} - a_{13} \cdot a_{22})$$

Substituindo os valores de (5) em (6) obtém-se

$$D = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} - 1 \cdot \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} + 1 \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \cdot 1 - 1 \cdot 1 + 1 \cdot 1 \quad (7)$$

$$D = 1$$

De acordo com a regra de Cramer, a solução para cada uma das variáveis é

$$X = \frac{D_X}{D}, \qquad Y = \frac{D_Y}{D}, \qquad Z = \frac{D_Z}{D}$$

$$D_X = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}, \qquad D_Y = \begin{vmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{vmatrix}, \qquad D_Z = \begin{vmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{vmatrix} \quad (8)$$

Substituindo os valores de (5) e o resultado de (7) em (8) obtém-se

$$D_X = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}, \qquad D_Y = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}, \qquad D_Z = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{vmatrix}$$

$$X = D_X = 0, \qquad Y = D_Y = 1, \qquad Z = D_Z = 0$$

Para o estudo de códigos de bloco lineares as operações polinomiais são de fundamental importância. Uma palavra binária pode ser representada por um polinômio na forma:

$$f(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_n X^n$$

Assim, a palavra binária (101011), onde o bit mais significativo é o bit mais à esquerda, pode ser descrita pelo polinômio

$$f(X) = 1 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5$$

$$f(X) = 1 + X + X^3 + X^5$$

A adição (ou subtração) de dois polinômios

$$a(X) = 1 + X + X^3 + X^5 \qquad \text{e} \qquad b(X) = 1 + X^2 + X^3 + X^4 + X^7$$

pode ser feita da forma

$$\begin{array}{r} 1 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5 + 0X^6 + 0X^7 \\ + \quad 1 + 0X + 1X^2 + 1X^3 + 1X^4 + 0X^5 + 0X^6 + 1X^7 \\ \hline 0 + 1X + 1X^2 + 0X^3 + 1X^4 + 1X^5 + 0X^6 + 1X^7 \end{array}$$

$$a(X) + b(X) = X + X^2 + X^4 + X^5 + X^7$$

A multiplicação dos mesmos polinômios $a(X)$ e $b(X)$ é obtida fazendo

$$\begin{array}{l} 1 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5 + 0X^6 + 0X^7 \\ \cdot \quad 1 + 0X + 1X^2 + 1X^3 + 1X^4 + 0X^5 + 0X^6 + 1X^7 \\ \hline 1 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5 + 0X^6 + 0X^7 \\ \qquad 1X^2 + 1X^3 + 0X^4 + 1X^5 + 0X^6 + 1X^7 + 0X^8 + 0X^9 \\ \qquad\quad 1X^3 + 1X^4 + 0X^5 + 1X^6 + 0X^7 + 1X^8 + 0X^9 + 0X^{10} \\ \qquad\qquad 1X^4 + 1X^5 + 0X^6 + 1X^7 + 0X^8 + 1X^9 + 0X^{10} + 0X^{11} \\ \qquad\qquad\qquad 1X^7 + 1X^8 + 0X^9 + 1X^{10} + 0X^{11} + 1X^{12} + 0X^{13} + 0X^{14} \\ \hline 1 + 1X + 1X^2 + 1X^3 + 0X^4 + 1X^5 + 1X^6 + 1X^7 + 0X^8 + 1X^9 + 1X^{10} + 0X^{11} + 1X^{12} + 0X^{13} + 0X^{14} \end{array}$$

$$a(X) \cdot b(X) = 1 + X + X^2 + X^3 + X^5 + X^6 + X^7 + X^9 + X^{10} + X^{12}$$

Evidentemente, se $a(X) = 0$, então e $a(X)\cdot b(X) = 0$

Pode-se verificar que os polinômios sobre $GF(2)$ satisfazem as seguintes condições:

1. Comutativa:
$$a(X)+b(X)=b(X)+a(X)$$
$$a(X)\cdot b(X)=b(X)\cdot a(X)$$
2. Associativa:
$$a(X)+[b(X)+c(X)]=[a(X)+b(X)]+c(X)$$
$$a(X)\cdot[b(X)\cdot c(X)]=[a(X)\cdot b(X)]\cdot c(X)$$
3. Distributiva:
$$a(X)\cdot[b(X)+c(X)]=[a(X)\cdot b(X)]+[a(X)\cdot c(X)]$$

A divisão entre um polinômio $f(X)$ e um polinômio $g(X)$, no caso em que $f(X)$ possui grau maior ou igual do que $g(X)$ e $g(X)$ não é zero, resulta em um quociente e um resto e a operação pode ser escrita na forma do *algoritmo de divisão de Euclides* como

$$f(X)=q(X)g(X)+r(X).$$

Se, por exemplo,

$$f(X) = X^6 + X^5 + X^4 + X + 1 \qquad \text{e} \qquad g(X) = X^3 + X + 1$$

Então a divisão de $f(X)$ por $g(X)$ pode ser feita conforme mostrada a seguir

$$\begin{array}{l|l} X^6+X^5+X^4+X+1 & X^3+X+1 \\ \cline{2-2} X^6+X^4+X^3 & X^3+X^2 \quad \text{(quociente)} \\ \cline{1-1} X^5+X^3+X+1 & \\ X^5+X^3+X^2 & \\ \cline{1-1} X^2+X+1 \quad \text{(resto)} & \end{array}$$

Veja outro exemplo:

$$\begin{array}{l|l} X^{12}+X^{10}+X^9+X^7+X^6+X^5+X^3+X^2+X+1 & X^7+X^4+X^3+X^2+1 \\ \cline{2-2} X^{12}+X^9+X^8+X^7+X^5 & X^5+X^3+X+1 \\ \cline{1-1} X^{10}+X^8+X^6+X^3+X^2+X+1 & \\ X^{10}+X^7+X^6+X^5+X^3 & \\ \cline{1-1} X^8+X^7+X^5+X^2+X+1 & \\ X^8+X^5+X^4+X^3+X & \\ \cline{1-1} X^7+X^4+X^3+X^2+1 & \\ X^7+X^4+X^3+X^2+1 & \\ \cline{1-1} 0 & \end{array}$$

Um polinômio $f(X)$ sobre $GF(2)$, com número par de termos, é divisível por $X + 1$.

- *Polinômio irredutível*: Um polinômio $p(X)$ sobre $GF(2)$ de grau m é dito irredutível sobre $GF(2)$ se ele não for divisível por nenhum outro polinômio sobre $GF(2)$ de grau menor que m mas maior que zero. Como exemplo, os polinômios

$$X^2 + X + 1;$$
$$X^3 + X + 1;$$
$$X^4 + X + 1.$$

  são irredutíveis. Para qualquer $m \geq 1$ existe um polinômio irredutível de grau m.

- Qualquer polinômio irredutível sobre $GF(2)$de grau m divide $X^{2^m-1} + 1$.

EXEMPLO 4

Considere o polinômio $X^3 + X + 1$. Então $X^{2^3-1} + 1 = X^7 + 1$ e verifica-se que

$$\begin{array}{l|l} X^7 + 1 & X^3 + X + 1 \\ \hline X^7 + X^5 + X^4 & X^4 + X^2 + X + 1 \\ \hline X^5 + X^4 + 1 & \\ X^5 + X^3 + X^2 & \\ \hline X^4 + X^3 + X^2 + 1 & \\ X^4 + X^2 + X & \\ \hline X^3 + X + 1 & \\ X^3 + X + 1 & \\ \hline 0 & \end{array}$$

* * *

- *Polinômio primitivo*: um polinômio irredutível $p(X)$ de grau m é dito primitivo se o menor positivo inteiro n para o $p(X)$ divide $X^n + 1$ é $n = 2^m - 1$. Por exemplo,

$$p(X) = X^4 + X + 1$$

  é irredutível e primitivo pois $p(X)$ divide $X^{15} + 1$ e nenhum $X^n + 1$ para $1 \leq n < 15$.

  Por outro lado,

$$p(X) = X^4 + X^3 + X^2 + X + 1$$

  é irredutível mas não é primitivo pois além de $p(X)$ dividir $X^{15} + 1$ ele também divide $X^5 + 1$.

Não é fácil reconhecer um polinômio primitivo. Para um dado m, pode haver mais do que um polinômio primitivo de grau m. A tabela apresentada a seguir apresenta apenas um polinômio primitivo para cada valor de m. Os polinômios apresentados são os que possuem o menor número de termos.

Tabela 1.1 - Lista de polinômios primitivos [1]

m	$p(X)$	m	$p(X)$
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{17}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

Uma propriedade útil de polinômios sobre $GF(2)$ é que

$$[f(X)]^{2^i} = [f(X)^{2^i}] \tag{1.1}$$

EXEMPLO 5

Considere o polinômio $f(X) = 1+X+X^3$. Então,

$$f(X^2) = 1+X^2+X^6$$

e

$$f^2(X) = (1+X+X^3)(1+X+X^3) = 1+X+X^3+X+X^2+X^4+X^3+X^4+X^6$$

$$f^2(X) = 1+X^2+X^6$$

Logo,

$$f^2(X) = f(X^2)$$

* * *

1.4. CONSTRUÇÃO DE CAMPOS DE GALOIS $GF(2^m)$

Considere os dois elementos 0 e 1 de $GF(2)$, um novo símbolo α e a operação multiplicação "$\cdot$". Logo,

$$\begin{aligned} &0\cdot 0 = 0, && \alpha^2 = \alpha\cdot\alpha,\\ &0\cdot 1 = 0, && \alpha^3 = \alpha\cdot\alpha\cdot\alpha,\\ &1\cdot 1 = 1, && \quad\vdots\\ &0\cdot\alpha = \alpha\cdot 0 = 0, && \alpha^j = \alpha\cdot\alpha\cdot\cdots\cdot\alpha \quad (j \text{ vezes}),\\ &1\cdot\alpha = \alpha\cdot 1 = 1, && \quad\vdots \end{aligned} \tag{1.2}$$

Da operação de multiplicação definida acima, tem-se que

$$\begin{aligned} &0\cdot\alpha^j = \alpha^j\cdot 0 = 0,\\ &1\cdot\alpha^j = \alpha^j\cdot 1 = \alpha^j,\\ &\alpha^i\cdot\alpha^j = \alpha^j\cdot\alpha^i = \alpha^{i+j}. \end{aligned} \tag{1.3}$$

Agora tem-se um conjunto de elementos sobre o qual uma operação "$\cdot$" é definida:

$$F = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^j, \cdots\}$$

Note que o elemento 1 é, muitas vezes, escrito como α^0.

Considere agora a condição sobre o elemento α de forma que o conjunto F contém somente 2^m elementos e está fechado sob multiplicação "$\cdot$" definida por (1.2). Seja $p(X)$ um polinômio primitivo de grau m sobre $GF(2)$. Admita que $p(\alpha) = 0$, ou seja, α é uma raiz de $p(X)$. Uma vez que $p(X)$ divide $X^{2^m-1}+1$, tem-se:

$$X^{2^m-1}+1 = q(X)p(X). \tag{1.4}$$

Substituindo X por α em (1.4),

$$\alpha^{2^m-1}+1 = p(\alpha)\cdot q(a) \quad\Rightarrow\quad \alpha^{2^m-1}+1 = q(a)\cdot 0 \quad\Rightarrow\quad \alpha^{2^m-1}+1 = 0,$$

e ainda

$$\alpha^{2^m-1} = 1 = \alpha^0. \tag{1.5}$$

Portanto, existe um elemento $\alpha^{2^m-2} \neq 0$, a partir do qual os elementos do conjunto F tornam-se repetitivos, ou seja, torna-se finito, contendo os seguintes elementos:

$$F^* = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}. \tag{1.6}$$

Uma vez que o subconjunto {0, 1} forma um subcampo de $GF(2^m)$, $GF(2)$ é um subcampo de $GF(2^m)$, também chamado de *base do campo* (*ground field*).

A construção de um Campo de Galois, a partir de um polinômio primitivo, resulta em dois tipos de representação para os seus elementos: a representação por potência mostrada em (1.6) e a representação polinomial, obtida na construção do campo, conforme mostrada no Exemplo 6.

EXEMPLO 6

Seja $m = 4$ e considere o polinômio primitivo sobre $GF(2)$, $p(X) = 1 + X + X^4$. Admitindo que α seja uma raiz do polinômio, então $p(\alpha) = 0$, ou seja,

$$0 = 1 + \alpha + \alpha^4 \quad \Rightarrow \quad \alpha^4 = 1 + \alpha$$

A partir da relação acima pode-se construir um $GF(2^4)$ como se segue:

$$\begin{aligned}
&\alpha^5 = \alpha \cdot \alpha^4 = \alpha(1+\alpha) = \alpha + \alpha^2 \\
&\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3 \\
&\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3 \\
&\alpha^8 = \alpha \cdot \alpha^7 = \alpha(1 + \alpha + \alpha^3) = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + 1 + \alpha = 1 + \alpha^2 \\
&\qquad \vdots \\
&\alpha^{2^m - 2} = \alpha^{14} = 1 + \alpha^3
\end{aligned}$$

Tabela 1.2 - $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$

REPRESENTAÇÕES					
POR POTÊNCIA	**POLINOMIAL**	**VETORIAL**	**POR POTÊNCIA**	**POLINOMIAL**	**VETORIAL**
0	0	(0000)	α^7	$1 + \alpha + \alpha^3$	(1101)
$\alpha^0 = 1$	1	(1000)	α^8	$1 + \alpha^2$	(1010)
α^1	α	(0100)	α^9	$\alpha + \alpha^3$	(0101)
α^2	α^2	(0010)	α^{10}	$1 + \alpha + \alpha^2$	(1110)
α^3	α^3	(0001)	α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0111)
α^4	$1 + \alpha$	(1100)	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1111)
α^5	$\alpha + \alpha^2$	(0110)	α^{13}	$1 + \alpha^2 + \alpha^3$	(1011)
α^6	$\alpha^2 + \alpha^3$	(0011)	α^{14}	$1 + \alpha^3$	(1001)

* * *

Note que pelo fato dos Campos de Galois serem finitos, algumas operações algébricas triviais são realizadas de forma singular se comparadas com as operações equivalentes da álgebra comum.

A adição entre dois elemento de campo é mais facilmente realizável com os elementos em sua representação polinomial, conforme mostrado no Exemplo 7.

EXEMPLO 7

Seja o $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$. A adição entre os elementos α^5 e α^7 é

$$\alpha^5 + \alpha^7 = \alpha + \alpha^2 + 1 + \alpha + \alpha^3 = 1 + \alpha^2 + \alpha^3 = \alpha^{13}$$

Ou seja,

$$\alpha^5 + \alpha^7 = \alpha^{13}.$$

* * *

A multiplicação entre elementos do campo é mais facilmente realizada com os elementos em sua representação por potência, observando que o campo termina com o elemento α^{2^m-2}, conforme (1.6), e que o próximo elemento seria $\alpha^{2^m-1} = 1 = \alpha^0$, conforme (1.5). Logo, na operação de multiplicação entre elementos de um campo, o expoente do elemento produto não deve exceder 2^m - 2, uma vez que elementos com expoentes maiores do que estes são elementos já existentes no campo. Assim, quando o expoente de um produto exceder 2^m - 2, deve-se reduzir o expoente para o expoente de um elemento pertencente ao campo e este expoente nada mais é do que o resto da divisão do expoente excedente por 2^m - 1. Veja Exemplo 8.

EXEMPLO 8

Seja o $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$. O elemento de ordem mais alta do campo é

$$\alpha^{2^m-2} = \alpha^{14}.$$

Considere agora os elementos α^7 e α^{12}. O produto entre esses dois elementos é

$$\alpha^7 \cdot \alpha^{12} = \alpha^{19}$$

Note que $\alpha^{19} > \alpha^{14}$ e assim, o expoente deve ser reduzido fazendo 19 ÷ (2^m - 1) = 19 ÷ 15 = 1 e o resto é 4. Logo,

$$\alpha^7 \cdot \alpha^{12} = \alpha^{19} = \alpha^4$$

* * *

A operação de divisão entre dois elementos do campo deve ser pode ser feita por meio do produto do dividendo pelo inverso do divisor, lembrando que

$$\alpha^i \cdot \alpha^{-j} = \alpha^i \cdot (\alpha^0 \cdot \alpha^{-j}) = \alpha^i \cdot (\alpha^{2^m-1} \cdot \alpha^{-j}).$$

EXEMPLO 9

Seja o $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$. A divisão de α^7 por α^{12}.é

$$\frac{\alpha^7}{\alpha^{12}} = \alpha^7 \cdot \alpha^{-12} = \alpha^7 \cdot (\alpha^{2^m-1} \cdot \alpha^{-12}) = \alpha^7 \cdot (\alpha^{15} \cdot \alpha^{-12}) = \alpha^{10}$$

Portanto,

$$\frac{\alpha^7}{\alpha^{12}} = \alpha^{10}.$$

* * *

1.5. PROPRIEDADES BÁSICAS DE UM CAMPO DE GALOIS $GF(2^m)$

A seguir são apresentadas algumas propriedades básicas importantes de um Campo de Galois $GF(2^m)$.

- **SOBRE AS RAÍZES DE UM POLINÔMIO**

Um polinômio com coeficientes de $GF(2)$ pode não ter raízes em $GF(2)$ mas ter raízes em um campo de extensão $GF(2^m)$.

EXEMPLO 10

$X^4 + X^3 + 1$ é irredutível sobre $GF(2)$, entretanto, ele tem raízes em $GF(2^4)$. Dos elementos de $GF(2^4)$ dados na Tabela 1.2, os elementos α^7, α^{11}, α^{13} e α^{14} são raízes de $X^4 + X^3 + 1$. Pode-se verificar isso, para α^7, fazendo

$$(\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = (1 + \alpha^2 + \alpha^3) + (\alpha^2 + \alpha^3) + 1 = 0$$

O mesmo se verifica para α^{11}, α^{13} e α^{14}. Pode-se verificar também que:

$$\begin{aligned}
&(X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) \\
&= [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}] \\
&= (X^2 + \alpha^8 X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12}) \\
&= X^4 + (\alpha^8 + \alpha^{16})X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)X + \alpha^{15} \\
&= X^4 + X^3 + 1
\end{aligned}$$

* * *

Seja $f(X)$ um polinômio com coeficientes de $GF(2)$. Se um elemento β de $GF(2^m)$ é uma raiz de $f(X)$, então o polinômio $f(X)$ também tem como raízes β^{2^l} para qualquer $l \geq 0$. O elemento β^{2^l} é chamado de *conjugado* de β.

Os 2^m - 1 elementos não zero de $GF(2^m)$ formam todas as raízes de $X^{2^m-1} + 1$

EXEMPLO 11

O polinômio $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ tem como raiz o elemento α^4, do $GF(2^4)$ apresentado na Tabela 1.2, conforme mostrado a seguir.

$$f(\alpha^4) = 1 + \alpha^{12} + \alpha^{16} + \alpha^{20} + \alpha^{24} = 1 + \alpha^{12} + \alpha + \alpha^5 + \alpha^9$$
$$= 1 + (1 + \alpha + \alpha^2 + \alpha^3) + \alpha + (\alpha + \alpha^2) + (\alpha + \alpha^3) = 0$$

Os conjugados de α^4 são

$$(\alpha^4)^2 = \alpha^8; \qquad (\alpha^4)^{2^2} = \alpha^{16} = \alpha; \qquad (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2$$

Note que $(\alpha^4)^{24} = \alpha^{64} = \alpha^4$. Assim, α^2, α, α^8 são raízes de $f(X) = 1 + X^3 + X^4 + X^5 + X^6$. Pode-se verificar ainda que α^5 e seu conjugado α^{10} são raízes de $f(X) = 1 + X^3 + X^4 + X^5 + X^6$. Portanto, $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ possui seis raízes.distintas no $GF(2^4)$ da Tabela 1.2.

* * *

- **SOBRE POLINÔMIOS MÍNIMOS**

Seja β um elemento em $GF(2^m)$, e seja e o menor inteiro não negativo tal que $\beta^{2^e} = \beta$. Então,

$$\phi(X) = \prod_{i=0}^{e-1} (X + \beta^{2^i}) \tag{1.7}$$

é um polinômio irredutível sobre $GF(2)$ e é chamado de polinômio mínimo de β.

O polinômio mínimo $\phi(X)$ de um elemento β em $GF(2^m)$ divide $X^{2^m-1} + 1$

EXEMPLO 12

Considere o $GF(2^4)$ gerado por $g(X) = 1 + X + X^4$. Seja $\beta = \alpha^3$. Os conjugados de β são:

$$\beta^2 = \alpha^6, \quad \beta^{2^2} = \alpha^{12}, \quad \beta^{2^3} = \alpha^{24} = \alpha^9$$

O polinômio mínimo de $\beta = \alpha^3$ é então

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9)$$
$$\phi(X) = [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}]$$
$$\phi(X) = (X^2 + \alpha^2 X + \alpha^9)(X^2 + \alpha^8 X + \alpha^6)$$
$$\phi(X) = X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15}$$
$$\phi(X) = X^4 + X^3 + X^2 + X + 1$$

* * *

Todos os polinômios mínimos dos elementos do $GF(2^4)$ gerado por $g(X) = 1 + X + X^4$ são apresentados na Tabela 1.3.

Tabela 1.3 - Polinômios mínimos dos elementos do $GF(2^4)$ gerado por $g(X) = 1 + X + X^4$

Raízes conjugadas	Polinômios mínimos
0	X
1	$X+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$

O grau e de um polinômio Se e é o menor inteiro tal que $\beta^{2^e} = \beta$, então e é também o grau do polinômio mínimo $\phi(X)$ de um elemento β em $GF(2^m)$. Além disso, $e \leq m$.

Em particular, o grau do polinômio mínimo de qualquer elemento em $GF(2^m)$ divide m. Note que todos os graus dos polinômios mínimos dos elementos do $GF(2^4)$ apresentados na Tabela 2.3 são são fatores de 4.

- **SOBRE ELEMENTOS PRIMITIVOS**

Na construção do campo de Galois $GF(2^m)$ foi utilizado um polinômio primitivo $p(X)$ de grau m e definido que o elemento α fosse uma raiz de $p(X)$. Uma vez que as potências de α geram todos os elementos não zero de $GF(2^m)$, α é um *elemento primitivo*.

Se β é um elemento primitivo em $GF(2^m)$, todos os seus conjugados $\beta^2, \beta^{2^2}, \cdots$ são também elementos primitivos de $GF(2^m)$.

EXEMPLO 13

Considere o campo de Galois $GF(2^4)$ dado pela Tabela 1.2. As potências de $\beta = \alpha^7$ são

$$\beta^0 = 1, \beta^1 = \alpha^7, \beta^2 = \alpha^{14}, \beta^3 = \alpha^{21} = \alpha^6, \beta^4 = \alpha^{28} = \alpha^{13},$$
$$\beta^5 = \alpha^{35} = \alpha^5, \beta^6 = \alpha^{42} = \alpha^{12}, \beta^7 = \alpha^{49} = \alpha^4, \beta^8 = \alpha^{56} = \alpha^{11},$$
$$\beta^9 = \alpha^{63} = \alpha^3, \beta^{10} = \alpha^{70} = \alpha^{10}, \beta^{11} = \alpha^{77} = \alpha^2, \beta^{12} = \alpha^{84} = \alpha^9,$$
$$\beta^{13} = \alpha^{91} = \alpha, \beta^{14} = \alpha^{98} = \alpha^8, \beta^{15} = \alpha^{105} = 1.$$

Observa-se claramente que as potências de $\beta = \alpha^7$ geram todos os elementos não zeros de $GF(2^7)$, assim $\beta = \alpha^7$ é um elemento primitivo de $GF(2^7)$. Os conjugados de $\beta = \alpha^7$ são

$$\beta^2 = \alpha^{14}, \beta^{2^2} = \alpha^{13}, \beta^{2^3} = \alpha^{11}$$

Pode-se verificar que eles são os elementos primitivos de $GF(2^m)$.

Se β é um elemento de ordem n em $GF(2m)$, todos os seus conjugados tem a mesma ordem n. Lembrar que n é o menor inteiro positivo tal que $\beta^n = 1$.

EXEMPLO 14

Considere o elemento α^5 em $GF(24)$ gerado por $p(X) = 1 + X + X^4$. Uma vez que $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$, então o único conjugado de α^5 é $(\alpha^5)^2 = \alpha^{10}$. Ambos α^5 e α^{10} tem ordem $n = 3$, pois $(\alpha^5)^3 = (\alpha^{10})^3 = 1$. O polinômio mínimo de α^5 é $X^2 + X + 1$, cujo grau é um fator de 4. Os conjugados de α^3 são α^6, α^9 e α^{12}. A ordem de todos eles é $n = 5$.

* * *

1.6. CÁLCULOS UTILIZANDO ARITMÉTICA DOS CAMPOS DE GALOIS *GF*(2^m)

Nesta seção serão apresentados alguns exemplos de cálculos usando aritmética sobre $GF(2^4)$.

EXEMPLO 15

Considere as equações lineares sobre $GF(2^4)$ gerado por $g(X) = 1 + X + X^4$.

$$X + \alpha^7 Y = \alpha^2 \tag{1.8}$$

$$\alpha^{12} X + \alpha^8 Y = \alpha^4 \tag{1.9}$$

Multiplicando (1.9) por α^3, obtém-se

$$X + \alpha^{11} Y = \alpha^7 \tag{1.10}$$

Somando (1.8) com (1.10) com o auxílio da Tabela 1.2, obtém-se

$$\begin{aligned} &(\alpha^7 + \alpha^{11})Y = \alpha^2 + \alpha^7 \\ &(1 + \alpha + \alpha^3 + \alpha + \alpha^2 + \alpha^3)Y = \alpha^2 + 1 + \alpha + \alpha^3 \\ &(1 + \alpha^2)Y = 1 + \alpha + \alpha^2 + \alpha^3 \\ &\alpha^8 Y = \alpha^{12} \quad \Rightarrow \quad Y = \alpha^{12} \cdot \alpha^{15-8} \quad \Rightarrow \quad Y = \alpha^{12} \cdot \alpha^7 \\ &Y = \alpha^4 \end{aligned} \tag{1.11}$$

Substituindo (1.11) em (1.8)

$$\begin{aligned} &X + \alpha^7 \cdot \alpha^4 = \alpha^2 \quad \Rightarrow \quad X = \alpha^2 + \alpha^{11} \quad \Rightarrow \quad X = \alpha^2 + \alpha + \alpha^2 + \alpha^3 \\ &X = \alpha + \alpha^3 \quad \Rightarrow \quad X = \alpha^9. \end{aligned}$$

Alternativamente o sistema de equações pode ser resolvido pela regra de Cramer:

$$X = \frac{\begin{vmatrix} \alpha^2 & \alpha^7 \\ \alpha^4 & \alpha^8 \end{vmatrix}}{\begin{vmatrix} 1 & \alpha^7 \\ \alpha^{12} & \alpha^8 \end{vmatrix}} = \frac{\alpha^{10} + \alpha^{11}}{\alpha^8 + \alpha^{19}} = \frac{1 + \alpha^3}{\alpha + \alpha^2} = \frac{\alpha^{14}}{\alpha^5} = \alpha^9,$$

$$Y = \frac{\begin{vmatrix} \alpha^1 & \alpha^2 \\ \alpha^{12} & \alpha^4 \end{vmatrix}}{\begin{vmatrix} 1 & \alpha^7 \\ \alpha^{12} & \alpha^8 \end{vmatrix}} = \frac{\alpha^4 + \alpha^{14}}{\alpha^8 + \alpha^{19}} = \frac{\alpha + \alpha^3}{\alpha + \alpha^2} = \frac{\alpha^9}{\alpha^5} = \alpha^4.$$

* * *

EXEMPLO 16

Admita que se deseje resolver a equação a seguir, sobre $GF(2^4)$ gerado por $g(X) = 1 + X + X^4$, apresentado na Tabela 2.1.

$$f(X) = X^2 + \alpha^7 X + \alpha = 0$$

Não é possível aplicar a fórmula quadrática porque ela requer uma divisão por 2 e, em $GF(2^4)$, $2 = 0$. Se $f(X) = 0$ tem alguma solução em $GF(2^4)$, a solução pode ser encontrada substituindo X, na equação, por todos os elementos do campo gerado por $g(X) = 1 + X + X^4$.

Procedendo assim encontra-se

$$f(\alpha^6) = (\alpha^6)^2 + \alpha^7 \cdot \alpha^6 + \alpha = \alpha^{12} + \alpha^{13} + \alpha = 0,$$
$$f(\alpha^{10}) = (\alpha^{10})^2 + \alpha^7 \cdot \alpha^{10} + \alpha = \alpha^5 + \alpha^2 + \alpha = 0.$$

Assim, α^6 e α^{10} são raízes de $f(X)$, e

$$f(X) = (X + \alpha^6)(X + \alpha^{10}) = X^2 + (\alpha^{10} + \alpha^6)X + \alpha = X^2 + \alpha^7 X + \alpha$$

Este é um procedimento de cálculo típico requerido para a decodificação de códigos tais como os BCH e Reed-Solomon.

* * *

1.7. ESPAÇOS VETORIAIS

Seja V conjunto de elementos sobre os quais uma operação adição binária, "+", é definida. Considere que uma operação multiplicação, "·", entre os elementos de um campo F e os elementos de V seja também definida. O conjunto V é um espaço vetorial sobre o campo F se as seguintes condições forem satisfeitas:

1. V é um grupo comutativo sob adição.
2. Para qualquer elemento a em F e qualquer elemento $\mathbf{v}$ em V, $a \bullet \mathbf{v}$ é um elemento em V.
3. Lei distributiva: para quaisquer elementos $\mathbf{v}$ e $\mathbf{u}$ em V e quaisquer elementos a e b em F,

$$a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}.$$
$$(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}.$$

4. Lei associativa: para qualquer $\mathbf{v}$ em V e quaisquer a e b em F,

$$(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v}).$$

5. Seja 1 o elemento unitário de F. Então, para qualquer $\mathbf{v}$ em V, $1 \cdot \mathbf{v} = \mathbf{v}$.

Os elementos de V são chamados *vetores*, e os elementos do campo são chamados *escalares*. A adição sobre V é chamada de *adição vetorial*, e a multiplicação que combina um escalar em F com um vetor em V é chamado *produto vetorial.* O elemento identidade aditivo de V é $\mathbf{0}$.

Algumas propriedades básicas de um espaço vetorial V sobre um campo F são:

1. Seja 0 o elemento zero do campo F. Para qualquer vetor $\mathbf{v}$ em V, $0 \cdot \mathbf{v} = 0$.
2. Para qualquer escalar c em F, $c \cdot 0 = 0$.
3. Para qualquer escalar c em F e qualquer vetor v em V, $(-c) \cdot \mathrm{v} = c \cdot (-\mathrm{v}) = -(c \cdot \mathbf{v})$. Isto é, $(-c) \cdot \mathbf{v}$ ou $c \cdot (-\mathbf{v})$ é o aditivo inverso do vetor $c \cdot \mathbf{v}$.

Considere uma seqüência ordenada de n componentes, $(a^0, a^1, \ldots, a^{n-1})$, onde cada elemento ai é um elemento do campo binário $GF(2)$, (i.e., $a^i = 0$ ou 1). Esta seqüência é geralmente chamada uma n-tupla sobre $GF(2)$. Como ai pode assumir dois valores distintos, pode-se construir 2^n n-tuplas distintas.

Seja V_n o conjunto das 2^n n-tuplas distintas sobre $GF(2)$. Uma adição, +, sobre V_n é definida da seguinte forma: para qualquer

$$\mathbf{u} = (u_0, u_1, \ldots . u_{n-1}) \qquad \text{e} \qquad \mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$$

em V_n,

$$\mathbf{u} + \mathbf{v} = (u_0 + v_0, u_1 + v_1, \ldots, u_{n-1} + v_{n-1}),$$

onde $u_i + v_i$ é uma operação adição módulo-2.

Claramente, $\mathbf{u} + \mathbf{v}$ é também uma n-tupla em $GF(2)$, consequentemente, V_n é fechado sob adição módulo-2, ou seja, V_n é um grupo comutativo sob adição. A n-tupla toda zero, $0 = (0, 0, \ldots, 0)$, é o elemento identidade aditivo. Admita uma n-tupla toda zero $\mathbf{z} = (0, 0, \ldots, 0)$. Para qualquer $\mathbf{v}$ em V_n,

$$\mathbf{v} + \mathbf{z} = (v_0 + z_0, v_1 + z_1, \ldots, v_{n-1} + z_{n-1}) = (v_0 + 0, v_1 + 0, \ldots, v_{n-1} + 0)$$

O elemento aditivo inverso de cada n-tupla é ela própria.

Uma multiplicação escalar de uma n-tupla em V_n por um elemento a em $GF(2)$ é como se segue.

Para qualquer

$$\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \text{ em } V_n,$$

e qualquer a de $GF(2)$,

$$a \cdot \mathrm{v} = a \cdot (v_0, v_1, \ldots, v_{n-1}) = (a \cdot v_0, a \cdot v_1, \ldots, a \cdot v_{n-1}) ,$$

onde $a \cdot v_i$ é uma operação multiplicação módulo-2. Claramente, $a \cdot (v_0, v_1, \ldots, v_{n-1})$ é também uma n-tupla em V_n. Se

$$a = 1,\ 1 \cdot (v_0, v_1, \ldots, v_{n-1}) = (1 \cdot v_0, 1 \cdot v_1, \ldots, 1 \cdot v_{n-1}) = (v_0, v_1, \ldots, v_{n-1}).$$

O conjunto V_n de todas as n-tuplas sobre $GF(2)$ formam um espaço vetorial sobre $GF(2)$.

EXEMPLO 17

Seja $n = 5$. O espaçõ vetorial V_5 de todas as 5-tuplas sobre $GF(2)$ consistem dos seguintes 32 vetores:

(00000), (00001), (00010), (00011), (00100), (00101), (00110), (00111),
(01000), (01001), (01010), (01011), (01100), (01101), (01110), (01111),
(10000), (10001), (10010), (10011), (10100), (10101), (10110), (10111),
(11000), (11001), (11010), (11011), (11100), (11101), (11110), (11111).

* * *

EXEMPLO 18

A soma de (10111) e (11001) é

$$(10111) + (11001) = (1+1, 0+1, 1+0, 1+0, 1+1) = (01110).$$

Usando a regra de multiplicação escalar definida anteriormente, obtém-se:

$$0 \cdot (11010) = (0\cdot1, 0\cdot1, 0\cdot0, 0\cdot1, 0\cdot0) = (00000).$$
$$1 \cdot (11010) = (1\cdot1, 1\cdot1, 1\cdot0, 1\cdot1, 1\cdot0) = (11010).$$

* * *

Se S é um subconjunto não vazio de um espaço vetorial V sobre um campo F, e ntão, S é um subespaço de V se as seguintes condições são satisfeitas:

1. Para qualquer dois vetores **u** e **v** em S, **u** + **v** é também um vetor em S.
2. Para qualquer elemento a em F e qualquer vetor **u** em S, $a \cdot$ **u** está também em S.

EXEMPLO 19

Considere o espaço vetorial V_5 de todas as n-tuplas sobre $GF(2)$ dado no Exemplo 18. O conjunto {(00000), (00111), (11010) e (11101)} é um subespaço vetorial de V_5 pois satisfaz as duas condições estabelecidas para tal.

* * *

Sejam $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$, k vetores num espaço vetorial V sobre um campo F. Seja $a_1, a_2, \ldots, a_k$, k escalares de F. A soma

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k$$

é chamada de *combinação linear* de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.

A soma de duas combinações lineares de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$,

$$(a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots\ a_k\mathbf{v}_k) + (b_1\mathbf{v}_1 + b_2\mathbf{v}_2 + \ldots\ b_k\mathbf{v}_k) = (a_1+b_1)\mathbf{v}_1 + (a_2+b_2)\mathbf{v}_2 + \ldots (a_k+b_k)\mathbf{v}_k,$$

é uma combinação linear de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.

O produto de um escalar c em F e uma combinação linear de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$,

$$c \cdot (a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k) = (c \cdot a_1)\mathbf{v}_1 + (c \cdot a_2)\mathbf{v}_2 + \ldots + (c \cdot a_k)\mathbf{v}_k,$$

é também uma combinação linear de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.

Se $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ k vetores em um espaço vetorial V sobre um campo F, então o conjunto de todas as combinações lineares $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$, formam um subespaço de V.

EXEMPLO 20

Considere o espaço vetorial V_5 de todas as n-tuplas sobre $GF(2)$ dado no Exemplo 12. A combinação linear de (00111) e (11101) são

$$\begin{aligned}
0 \cdot (00111) + 0 \cdot (11101) &= (00000)\\
0 \cdot (00111) + 1 \cdot (11101) &= (11101)\\
1 \cdot (00111) + 0 \cdot (11101) &= (00111)\\
1 \cdot (00111) + 1 \cdot (11101) &= (11010)
\end{aligned}$$

Estes quatro vetores formam o mesmo subespaço vetorial do Exemplo 19.

* * *

Um conjunto de vetores $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ em um espaço vetorial V sobre um campo F é dito ser linearmente dependente se e somente se existem k escalares $a_1, a_2, \ldots, a_k$ de F, não todo zero, tal que $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k = 0$.

Um conjunto de vetores $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ é dito ser linearmente independente se ele não é linearmente dependente. Isto é, se $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ são linearmente independentes, então

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k \neq 0.$$

Exceto, $a_1 = a_2 = \ldots = a_k = 0$.

EXEMPLO 21

Os vetores (10110), (01001), e (11111) são linearmente dependes, uma vez que

$$1\cdot(10110) + 1\cdot(01001) + 1\cdot(11111) = (00000);$$

entretanto, os vetores (10110), (01001), e (11011) são linearmente independentes. Todas as oito combinações lineares desses vetores são apresentadas a seguir.

$$\begin{aligned}
&0\cdot(10110) + 0\cdot(01001) + 0\cdot(11011) = (00000),\\
&0\cdot(10110) + 0\cdot(01001) + 1\cdot(11011) = (11011),\\
&0\cdot(10110) + 1\cdot(01001) + 0\cdot(11011) = (01001),\\
&0\cdot(10110) + 1\cdot(01001) + 1\cdot(11011) = (10010),\\
&1\cdot(10110) + 0\cdot(01001) + 0\cdot(11011) = (10110),\\
&1\cdot(10110) + 0\cdot(01001) + 1\cdot(11011) = (01101),\\
&1\cdot(10110) + 1\cdot(01001) + 0\cdot(11011) = (11111),\\
&1\cdot(10110) + 1\cdot(01001) + 1\cdot(11011) = (00100).
\end{aligned}$$

* * *

Considere o espaço vetorial V_n de todas as n-tuplas sobre $GF(2)$. Considere as n-tuplas $\mathbf{e}_i$ que possuem um único elemento não zero na i-ésima posição, conforme mostrado a seguir.

$$\begin{aligned}
\mathbf{e}_0 &= (1, 0, 0, 0, \ldots , 0, 0),\\
\mathbf{e}_1 &= (0, 1, 0, 0, \ldots , 0, 0),\\
&\vdots\\
\mathbf{e}_{n-1} &= (0, 0, 0, 0, \ldots , 0, 1).
\end{aligned}$$

As n-tuplas $\mathbf{e}_i$ são linearmente independentes e todas as 2^n n-tupla $(a_0, a_1, a_2, \ldots , a_{n-1})$ em V_n podem ser obtidas a partir de combinações lineares de $\mathbf{e}_i$, como se segue.

$$(a_0, a_1, a_2, \ldots , a_{n-1}) = a_0\mathbf{e}_0 + a_1\mathbf{e}_2 + a_2\mathbf{e}_2 + \ldots + a_{n-1}\mathbf{e}_{n-1}.$$

Portanto, as n-tuplas $\mathbf{e}_i$ formam uma base do espaço vetorial V_n, cuja dimensão é n.

Se $k < n$ e $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ são k vetores linearmente independentes em V_n , então todas as combinações lineares de $\mathbf{v}_1$, $\mathbf{v}_2$, ... , $\mathbf{v}_k$ da forma

$$\mathbf{u} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \ldots + c_k\mathbf{v}_k$$

formam um subsespaço S de V_n , k-dimensional, ou seja, existem 2^k possíveis versões distintas de $\mathbf{v}_i$.

Seja $\mathbf{u} = (u_0, u_1, \ldots , u_{n-1})$ e $\mathbf{v} = (v_0, v_1, \ldots , v_{n-1})$ duas n-tuplas em V_n. O produto interno de **u** e **v** é definido como

$$\mathbf{u} \cdot \mathbf{v} = u_0 v_0 + u_1 v_1 + \ldots + u_{n-1} v_{n-1} ,$$

onde as adições e produtos são operações módulo-2. Assim, o produto interno $\mathbf{u} \cdot \mathbf{v}$ é um escalar em $GF(2)$. Se $\mathbf{u} \cdot \mathbf{v} = 0$**,** **u** e **v** são ditos ortogonais entre si.

O produto interno tem as seguintes propriedades:

1. $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$**.**
2. $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$.
3. $(a\mathbf{u}) \cdot \mathbf{v} = a(\mathbf{u} \cdot \mathbf{v})$.

Seja S um subespaço k-dimensional de V_n e S_d um conjunto de vetores em V_n tal que para qualquer **u** em S e **v** em S_d , $\mathbf{u} \cdot \mathbf{v} = 0$. O conjunto S_d contém pelo menos a n-tupla toda zero $\mathbf{0} = (0, 0, \ldots , 0)$, uma vez que para qualquer **u** em S, $\mathbf{0} \cdot \mathbf{u} = 0$. Assim, para qualquer elemento a em $GF(2)$ e qualquer **v** em S_d Portanto, $a \cdot \mathbf{v}$ está também em S_d.

Seja **v** e **w** quaisdquer dois vetores em S_d. Para qualquer vetor **u** em S,

$$\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} = 0 + 0 = 0.$$

Isso significa que se **v** e **w** são ortogonais a **u**, o vetor **v** + **w** é também ortogonal a **u**. Consequentemente, **v** + **w** é um vetor em S_d. Desta forma, S_d é também um subespaço vetorial de V_n. Este subespaço S_d é chamado de espaço nulo ou espaço dual de S.

Se S um subespaço vetorial do espaço vetorial V_n de todas as n-tuplas sobre $GF(2)$, a dimensão do seu espaço nulo S_d é $n - k$. Em outras palavras,

$$\dim (S) + \dim (S_d) = n.$$

EXEMPLO 22

Considere o espaço vetorial V_5 de todas as n-tuplas sobre $GF(2)$ do Exemplo 12. Os oito vetores seguintes formam um subespaço tridimensional S de V_5.

(00000), (11100), (01010), (10001), (10110), (01101), (11011), (00111).

O espaço nulo S_d de S consiste dos seguintes quatro vetores:

(00000), (10101), (01110), (11011).

S_d pode ser construído a partir dos vetores (10101) e (01110) que são linearmente independentes. Assim, a dimensão de S_d é 2.

* * *

1.8. MATRIZES

Uma matriz $k \times n$ sobre $GF(2)$ é um arranjo retangular com k linhas e n colunas,

$$\mathbf{G} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & & & & \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

onde cada $g_{i,j}$ com $0 \le i < k$ e $0 \le j < n$ é um elemento do campo binário $GF(2)$. A matriz **G** pode também ser representada pelas suas k linhas $\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}$ como se segue

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix}$$

Se as k ($k \le n$) linhas de **G** são linearmente independentes, então as 2^k combinações das linhas formam um subespaço k-dimensional do espaço vetorial V_n.

A troca de posições das linhas de **G** ou soma de uma linha com uma outra constituem o que é chamado de operações elementares de linhas. Fazendo operações elementares nas linhas de **G** pode-se obter uma outra matriz **G'** que gera o mesmo subespaço k-dimensional.

EXEMPLO 23

Considere uma matriz **G,** 3×6, sobre $GF(2)$,

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Somando a terceira linha com a primeira e trocando a terceira linha com a segunda, obtém-se

$$\mathbf{G'} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Ambas as matrizes **G** e **G'** geram o seguinte subespaço

(000000), (100101), (010011), (001110),(110110), (101011), (011101), (111000).

Este é um subespaço tridimensional do espaço vetorial V_6 de todas as 6-tuplas sobre $GF(2)$.

* * *

Se existe um subespaço S gerado por **G,** $k \times n$, sobre $GF(2)$, então existe um subespaço S_d cuja dimensão é $n - k$. Sejam $\mathbf{h}_0$, $\mathbf{h}_1$, ... , $\mathbf{h}_{n-k-1}$ vetores linearmente independentes de S_d. Se esses vetores geram S_d então pode-se formar uma matriz **H**, $(n - k) \times n$, usando $\mathbf{h}_0$, $\mathbf{h}_1$, ... , $\mathbf{h}_{n-k-1}$ como linhas:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{00} & h_{01} & \cdots & h_{0,n-1} \\ h_{10} & h_{11} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix}$$

Devido ao fato de que cada linha $\mathbf{g}_i$ de **G** é um vetor em S, e cada linha $\mathbf{h}_j$ de **H** é um vetor em S_d, o produto interno de $\mathbf{g}_i$ e $\mathbf{h}_j$ deve ser zero ($\mathbf{g}_i \cdot \mathbf{h}_j = 0$).

Para qualquer matriz **G**, $k \times n$, sobre $GF(2)$, com k linhas linearmente independentes, existe uma matriz **H**, $(n - k) \times n$, sobre $GF(2)$ com $n - k$ linhas linearmente independentes tal que para qualquer linha em $\mathbf{g}_i$ em **G** e qualquer linha $\mathbf{h}_j$ em **H**, $\mathbf{g}_i \cdot \mathbf{h}_j = 0$. O subespaço gerado por **G** é o espaço nulo gerado por **H** e vice-versa.

EXEMPLO 24

Considere a seguinte matriz 3×6, sobre $GF(2)$:

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

A matriz que gera o espaço nulo do subespaço gerado por **G** é

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Pode-se verificar facilmente que cada linha de **G** é ortogonal a cada linha de **H** e vice-versa.

* * *

Duas matrizes podem ser somadas se elas possuírem o mesmo número de linhas e o mesmo número de colunas. Se $\mathbf{A} = [a_{ij}]$ e $\mathbf{B} = [b_{ij}]$ são matrizes $k \times n$, então $[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$ que também é uma matriz $k \times n$.

Duas matrizes podem ser multiplicadas desde que o número de colunas da primeira matriz seja igual ao número de linhas da segunda matriz. Se $\mathbf{A} = [a_{ij}]$ é uma matriz $k \times n$ e $\mathbf{B} = [b_{ij}]$ é uma matriz $k \times l$, então $\mathbf{C} = \mathbf{A} \times \mathbf{B} = [c_{ij}]$.

Na matriz resultante $k \times l$, c_{ij} é igual ao produto interno da i-ésima linha $\mathbf{a}_i$ em **A** e a j-ésima coluna $\mathbf{b}_j$ em **B**; isto é

$$c_{ij} = \mathbf{a}_i \cdot \mathbf{b}_j = \sum_{t=0}^{n-1} a_{it} b_{tj}$$

Seja **G** uma matriz $k \times n$ sobre $GF(2)$. A matriz transposta de **G**, denotada por $\mathbf{G}^T$, é uma matriz $n \times k$ cujas linhas são colunas de **G** e cujas colunas são linhas de **G**.

Uma matriz $k \times k$, denotada por $\mathbf{I}_k$, é chamada de matriz identidade se ela tem 1's na sua diagonal principal e o resto é zero.

Uma submatriz de uma matriz **G** é uma matriz que foi obtida por descarte de determinadas linhas ou colunas de **G**.

1.9. EXERCÍCIOS

1. Resolva o sistema de equações abaixo utilizando aritmética módulo-2.

$$\begin{aligned} X + Y + W &= 1 \\ X + Z + W &= 0 \\ X + Y + Z + W &= 1 \\ Y + Z + W &= 0 \end{aligned}$$

2. Mostre que $X^5 + X^3 + 1$ é irredutível sobre $GF(2)$.

3. Encontre todos os polinômios irredutíveis de grau 5 sobre $GF(2)$.

4. Construa uma tabela para $GF(2^3)$ a partir do polinômio primitivo $p(X) = 1 + X + X^3$, mostrando todos os elementos em sua forma de potência, polinomial e vetorial. Encontre a ordem de todos os elementos.

5. Construa uma tabela para $GF(2^5)$ a partir do polinômio primitivo $p(X) = 1 + X^2 + X^5$. Seja α um elemento primitivo de $GF(2^5)$. Encontre os polinômios mínimos de α^3 e α^7.

6. Seja α um elemento primitivo de $GF(2^5)$. Use a Tabela 1.1 para encontrar as raízes do polinômio $f(X) = X^3 + \alpha^6 X^2 + \alpha^9 X + \alpha^9$.

7. Seja α um elemento primitivo de $GF(2^4)$. Divida o polinômio $f(X) = \alpha^3 X^7 + \alpha X^6 + \alpha^7 X^4 + \alpha^2 X^2 + \alpha^{11} X + 1$ sobre $GF(2^4)$ pelo polinômio $g(X) = X^4 + \alpha^3 X^2 + \alpha^5 X + 1$ sobre $GF(2^4)$. Encontre o quociente e o resto (use a Tabela 1.1).

8. Seja α um elemento primitivo de $GF(2^4)$. Use a Tabela 1.1 para resolver o sistema de equações abaixo.

$$X + \alpha^5 Y + Z = \alpha^7$$
$$X + \alpha Y + \alpha^7 Z = \alpha^9$$
$$\alpha^2 X + Y + \alpha^6 Z = \alpha$$

9. Dadas as matrizes

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

10. Encontre um subespaço vetorial tridimensional de V_5 sobre $GF(2)$ e determine seu espaço nulo.

1.10. Referência Bibliográfica

[1] LIN, S.; COSTELO JR, D. J. *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs: Prentice Hall, 1983. ISBN 013283796X.

ANEXO 1.1

TABELAS DE $GF(2^m)$ PARA $1 < m < 8$ [1]

Os elementos dos campos apresentados nas tabelas a seguir estão representados em sua forma vetorial, antecedido pela potência do elemento. O bit mais à direita da palavra binária é o bit de ordem mais alta do vetor. Por exemplo, em $GF(2^4)$ o elemento α^7 é representado como

7	1101

Que na forma polinomial fica $1 + \alpha + \alpha^3$. Ou seja, $\alpha^7 = 1 + \alpha + \alpha^3$.

1. $GF(2^3)$ gerado por $p(X) = 1 + X + X^3$

-	000	0	100	1	010	2	001
3	110	4	011	5	111	6	101

2 $GF(2^4)$ gerado por $p(X) = 1 + X + X^4$

-	0000	0	1000	1	0100	2	0010
3	0001	4	1100	5	0110	6	0011
7	1101	8	1010	9	0101	10	1110
11	0111	12	1111	13	1011	14	1001

3. $GF(2^5)$ gerado por $p(X) = 1 + X^2 + X^5$

-	00000	0	10000	1	01000	2	00100
3	00010	4	00001	5	10100	6	01010
7	00101	8	10110	9	01011	10	10001
11	11100	12	01110	13	00111	14	10111
15	11111	16	11011	17	11001	18	11000
19	01100	20	00110	21	00011	22	10101
23	11110	24	01111	25	10011	26	11101
27	11010	28	01101	29	10010	30	01001

4. $GF(2^6)$ gerado por $p(X) = 1 + X + X^6$

-	000000	0	100000	1	010000	2	001000
3	000100	4	000010	5	000001	6	110000
7	011001	8	001100	9	000110	10	000011
11	110001	12	101000	13	010100	14	001010
15	000101	16	110010	17	011001	18	111100
19	011110	20	001111	21	110111	22	101011
23	100101	24	100010	25	010001	26	111000
27	011100	28	001110	29	000111	30	110011

4. $GF(2^6)$ gerado por $p(X) = 1 + X + X^6$ (continuação)

31	101001	32	100100	33	010010	34	001001
35	110100	36	011010	37	001101	38	110110
39	011011	40	111101	41	101110	42	010111
43	111011	44	101101	45	100110	46	010011
47	111001	48	101100	49	010110	50	001011
51	110101	52	101010	53	010101	54	111010
55	011101	56	111110	57	011111	58	111111
59	101111	60	100111	61	100011	62	100001

5. $GF(2^7)$ gerado por $p(X) = 1 + X^3 + X^7$

-	0000000	0	1000000	1	0100000	2	0010000
3	0001000	4	0000100	5	0000010	6	0000001
7	1001000	8	0100100	9	0010010	10	0001001
11	1001100	12	0100110	13	0010011	14	1000001
15	1101000	16	0110100	17	0011010	18	0001101
19	1001110	20	0100111	21	1011011	22	1100101
23	1111010	24	0111101	25	1010110	26	0101011
27	1011101	28	1100110	29	0110011	30	1010001
31	1100000	32	0110000	33	0011000	34	0001100
35	0000110	36	0000011	37	1001001	38	1101100
39	0110110	40	0011011	41	1000101	42	1101010
43	0110101	44	1010010	45	0101001	46	1011100
47	0101110	48	0010111	49	1000011	50	1101001
51	1111100	52	0111110	53	001111	54	1000111
55	1101011	56	1111101	57	1110110	58	0111011
59	1010101	60	1100010	61	0110001	62	1010000
63	0101000	64	0010100	65	0001010	66	0000101
67	1001010	68	0100101	69	1011010	70	0101101
71	1011110	72	0101111	73	1011111	74	1100111
75	1111011	76	1110101	77	1110010	78	0111001
79	1010100	80	0101010	81	0010101	82	1000010
83	0100001	84	1011000	85	0101100	86	0010110
87	0001011	88	1001101	89	1101110	90	0110111
91	1010011	92	1100001	93	1111000	94	0111100
95	0011110	96	0001111	97	1001111	98	1101111
99	1111111	100	1110111	101	1110011	102	1110001
102	1110000	104	0111000	105	0011100	106	0001110
107	0000111	108	1001011	109	1101101	110	1111110
111	0111111	112	1010111	113	1100011	114	1111001
115	1110100	116	0111010	117	0011101	118	1000110
119	0100011	120	1011001	121	1100100	122	0110010
123	0011001	124	1000100	125	0100010	126	0010001

6. $GF(2^8)$ gerado por $p(X) = 1 + X^2 + X^3 + X^4 + X^8$

-	00000000	0	10000000	1	01000000	2	00100000
3	00010000	4	00001000	5	00000100	6	00000010
7	00000001	8	10111000	9	01011100	10	00101110
11	00010110	12	10110011	13	11100001	14	11001000
15	01100100	16	00110010	17	00011001	18	10110100
19	01011010	20	00101101	21	10101110	22	01010111
23	10010011	24	11110001	25	11000000	26	01100000
27	00110000	28	00011000	29	00001100	30	00000110
31	00000011	32	10111001	33	11100100	34	01110010
35	00111001	36	10100100	37	01010010	38	00101001
39	10101100	40	01010110	41	00101011	42	10101101
43	11101110	44	01110111	45	10000011	46	11111001
47	11000100	48	01100010	49	00110001	50	10100000
51	01010000	52	00101000	53	00010100	54	00001010
55	00000101	56	10111010	57	01011101	58	10010110
59	01001011	60	10011101	61	11110110	62	01111011
63	10000101	64	11111010	65	01111101	66	10000110
67	01000011	68	10011001	69	11110100	70	01111010
71	00111101	72	10100110	73	01010011	74	10010001
75	11110000	76	01111000	77	00111100	78	00011110
79	00001111	80	10111111	81	11100111	82	11001011
83	11011101	84	11010110	85	01101011	86	10001101
87	11111110	88	01111111	89	10000111	90	11111011
91	11000101	92	11011010	93	01101101	94	10001110
95	01000111	96	10011011	97	11110101	98	11000010
99	01100001	100	10001000	101	01000100	102	00100010
103	00010001	104	10110000	105	01011000	106	00101100
107	00010110	108	00001011	109	10111101	110	11100110
111	01110011	112	10000001	113	11111000	114	01111100
115	00111110	116	00011111	117	10110111	118	11100011
119	11001001	120	11011100	121	01101110	122	00110111
123	10100011	124	11101001	125	11001100	126	01100110
127	00110011	128	10100001	129	11101000	130	01110100
131	00111010	132	00011101	133	10110110	134	01011011
135	10010101	136	11110010	137	01111001	138	10000100
139	01000010	140	00100001	141	10101000	142	01010100
143	00101010	144	00010101	145	10110010	146	01011001
147	10010100	148	01001010	149	00100101	150	10101010
151	01010101	152	10010010	153	01001001	154	10011100
155	01001110	156	00100111	157	10101011	158	11101101
159	11001110	160	01100111	161	10001011	162	11111101
163	11000110	164	01100011	165	10001001	166	11111100
167	01111110	168	00111111	169	10100111	170	11101011

6. $GF(2^8)$ gerado por $p(X) = 1 + X^2 + X^3 + X^4 + X^8$ (continuação)

171	11001101	172	11011110	173	01101111	174	10001111
175	11111111	176	11000111	177	11011011	178	11010101
179	11010010	180	01101001	181	10001100	182	01000110
183	00100011	184	10101001	185	11101100	186	01110110
187	01111011	188	10100101	189	11101010	190	01110101
191	10000010	192	01000001	293	10011000	194	01001100
195	00100110	196	00010011	197	10110001	198	11100000
199	01110000	200	00111000	201	00011100	202	00001110
203	00000111	204	10111011	205	11100101	206	11001010
207	01100101	208	10001010	209	01000101	210	10011010
211	01001101	212	10011110	213	01001111	214	10011111
215	11110111	216	11000011	217	11011011	218	11010100
219	01101010	220	00110101	221	10100010	222	01010001
223	10010000	224	01001000	225	00100100	226	00010010
227	00001001	228	10111100	229	01011110	230	00101111
231	10101111	232	11101111	233	11001111	234	11011111
235	11010111	236	11010011	237	11010001	238	11010000
239	01101000	240	00110100	241	00011010	242	00001101
243	10100010	244	01011111	245	10010000	246	11110011
247	11000001	248	11011000	249	01101100	250	00110110
251	00011011	252	10110101	253	11100010	254	01110001