Capítulo 5

Campos finitos

5.1. Introducción

Presentaremos algunos conceptos básicos de la teoría de los campos finitos. Para mayor información, consultar el texto de McEliece [61] o el de Lidl y Niederreiter [58].

Un *campo finito* consiste de un conjunto finito de elementos F sobre el cual se definen un par de operaciones binarias $+$ y $\cdot$, las cuales satisfacen las siguientes propiedades aritméticas:

1. $(F, +)$ es un grupo abeliano, denominado el *grupo aditivo* del campo.

2. $(F^* = F - 0, \cdot)$ es un grupo abeliano, al que se denomina *grupo multiplicativo* del campo.

3. El producto tiene la propiedad *distributiva* respecto de la suma, esto es, $a \cdot (b + c) = a \cdot b + a \cdot c$.

El *orden* de un campo finito es el número de elementos en el campo. Existe un campo finito de orden q si y solo si q es la potencia de un número primo. Si q es la potencia de un primo, existe esencialmente un solo campo finito de orden q al cual denotaremos como $GF(q)$. Existen, sin embargo, varias maneras de representar a los elementos de $GF(q)$. Algunas de estas representaciones darán origen a implementaciones más eficientes de la aritmética del campo.

Si $q = p^m$ donde p es un primo y m un entero positivo, entonces p es denominado la *característica* del campo $GF(q)$ y m es denominado el *grado de extensión* de $GF(q)$.

5.2. El campo finito $GF(p)$

Sea p un número primo. El campo $GF(p)$, denominado un *campo primo*, está compuesto por el conjunto de enteros $\{0, 1, \ldots, p-1\}$ con las siguientes operaciones aritméticas:

- Adición: Si $a, b \in GF(p)$, entonces $a + b = r$, donde r es el residuo de la división de $a+b$ entre p y $0 \leq r \leq p-1$. Esta operación es conocida como la *suma módulo p*.
- Multiplicación: Si $a, b \in GF(p)$, entonces $a \cdot b = s$, donde s es el residuo de la división de $a \cdot b$ entre p. A esta operación se le conoce como *multiplicación módulo p*.
- Inversión: Si a un elemento de $GF(p)$ diferente de cero, el *inverso* de a módulo p, denotado como a^{-1}, es el entero único $c \in GF(p)$ tal que $a \cdot c = 1$.

Ejemplo 5.1 *El campo finito* $GF(23)$. Los elementos de $GF(23)$ son

$$\{0, 1, 2, \ldots, 22\}.$$

Ejemplos de operaciones aritméticas sobre $GF(23)$ son:

- $12 + 20 = 9$.
- $8 \cdot 9 = 3$.
- $8^{-1} = 3$.

El elemento 5 es un generador de $GF(23)$. Las potencias de 5 son:

$5^0 = 1$	$5^1 = 5$	$5^2 = 2$	$5^3 = 10$	$5^4 = 4$	$5^5 = 20$
$5^6 = 8$	$5^7 = 17$	$5^8 = 16$	$5^9 = 11$	$5^{10} = 9$	$5^{11} = 22$
$5^{12} = 18$	$5^{13} = 21$	$5^{14} = 13$	$5^{15} = 19$	$5^{16} = 3$	$5^{17} = 15$
$5^{18} = 6$	$5^{19} = 7$	$5^{20} = 12$	$5^{21} = 14$	$5^{22} = 1$.	

Ejemplo 5.2 *El campo finito* $GF(9395745580217015633)$ Algunos ejemplos de operaciones aritméticas sobre $GF(p)$ donde p es el número primo 9395745580217015633, son las siguientes:[1]

[1]Los cálculos de este ejemplo fueron realizados utilizando la libreria NTL (*Number Theoretical Library*) de Victor Shoup, disponible en http://www.shoup.net/ntl/

- $7340302972543780972 + 5581361980363885816$
  $= 3525919372690651155.$
- $7340302972543780972 * 5581361980363885816$
  $= 9209369511873859808.$
- $7340302972543780972^{-1} = 235766344840814111.$
- $(7340302972543780972)^4 = 4365113207684101270.$
- $(7340302972543780972)^5 = 3041767439943718402.$

5.3. El campo finito $GF(2^m)$

El campo $GF(2^m)$, denominado un *campo finito de característica dos* o *campo finito binario*, puede ser visto como un espacio vectorial de dimensión m sobre el campo $GF(2)$. Esto es, existen m elementos $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ en $GF(2^m)$ tales que cada elemento $\alpha \in GF(2^m)$ puede ser escrito en forma única como:

$$\alpha = a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{m-1}\alpha_{m-1},$$

donde $a_i \in \{0, 1\}$. Al conjunto $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ se le denomina una *base* de $GF(2^m)$ sobre $GF(2)$. Dada una base tal, un elemento α del campo puede ser representado por la cadena de bits $(a_0a_1 \cdots a_{m-1})$. La adición de elementos en el campo se realiza mediante el XOR bit a bit de sus representaciones vectoriales.

Existen diferentes bases de $GF(2^m)$ sobre $GF(2)$. Algunas bases dan origen a implementaciones más eficientes en hardware o software de la aritmética sobre $GF(2^m)$. El estándar ANSI X9.62 [4] permite dos tipos de bases: las *bases polinomiales* y las *bases normales*.

5.3.1. Representación en bases polinomiales

Sea

$$f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_2x^2 + f_1x + f_0,$$

donde $f_i \in \{0, 1\}$ para $i = 0, 1, \ldots, m-1$, un polinomio irreducible de grado m sobre $GF(2)$. Entonces $f(x)$ define una representación de base polinomial de $GF(2^m)$, la cual describiremos a continuación.

El campo $GF(2^m)$ está compuesto por todos los polinomios sobre $GF(2)$ de grado menor a m,

$$GF(2^m) = \left\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 \ : \ a_i \in \{0, 1\}\right\}.$$

Al elemento $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$ usualmente se le denota por la cadena de bits $(a_{m-1}a_{m-2}\cdots a_1a_0)$ de longitud m, de modo que

$$GF(2^m) = \{(a_{m-1}a_{m-2}\cdots a_1a_0) \ : \ a_i \in \{0,1\}\}.$$

Se define entonces las siguientes operaciones aritméticas sobre los elementos de $GF(2^m)$ cuando se tiene una representación de base polinomial con reducción polinomial $f(x)$:

- Adición: Si $(a_{m-1}a_{m-2}\cdots a_1a_0)$ y $(b_{m-1}b_{m-2}\cdots b_1b_0)$ son elementos de $GF(2^m)$, entonces $a + b = c = (c_{m-1}c_{m-2}\cdots c_1c_0)$ donde $c_i = a_i + b_i \bmod 2$.
- Multiplicación: Si $(a_{m-1}a_{m-2}\cdots a_1a_0)$ y $(b_{m-1}b_{m-2}\cdots b_1b_0)$ son elementos de $GF(2^m)$, entonces $a \cdot b = r = (r_{m-1}r_{m-2}\cdots r_1r_0)$ donde el polinomio $r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \cdots + r_1x + r_0$ es el residuo de la división de

  $$(a_{m-1}x^{m-1} + \cdots + a_1x + a_0) \cdot (b_{m-1}x^{m-1} + \cdots + b_1x + b_0)$$

  entre $f(x)$.
- Inversión: Si a es un elemento de $GF(2^m)$ diferente de cero, el *inverso* de a, denotado por a^{-1}, es el elemento $c \in GF(2^m)$ tal que $c \cdot a = 1$.

Ejemplo 5.3 *Una representación en base polinomial para* $GF(2^4)$. Sea

$$f(x) = x^4 + x + 1.$$

la reducción polinomial. Entonces los 16 elementos de $GF(2^4)$ son:

0 (0000)	1 (0001)	x (0010)	$x+1$ (0011)
x^2 (0100)	x^2+1 (0101)	x^2+x (0110)	x^2+x+1 (0111)
x^3 (1000)	x^3+1 (1001)	x^3+x (1010)	x^3+x+1 (1011)
x^3+x^2 (1100)	x^3+x^2+1 (1101)	x^3+x^2+x (1110)	x^3+x^2+x+1 (1111)

Algunos ejemplos de operaciones aritméticas sobre $GF(2^4)$ son:

- $(1101) + (1001) = (0100)$.

- $(1101)\cdot(1001) = (1111)$ dado que $(x^3+x^2+1)\cdot(x^3+1) = x^6+x^5+x^2+1$ y $(x^6+x^5+x^2+1)$ mód $(x^4+x+1) = x^3+x^2+x+1$.
- $(1101)^{-1} = (0100)$.

El elemento $\alpha = x = (0010)$ es un generador del grupo multiplicativo $GF(2^4)^*$, dado que es de orden 15 como se muestra en el siguiente cálculo:

$\alpha^1 = (0010)$	$\alpha^2 = (0100)$	$\alpha^3 = (1000)$	$\alpha^4 = (0011)$	$\alpha^5 = (0110)$
$\alpha^6 = (1100)$	$\alpha^7 = (1011)$	$\alpha^8 = (0101)$	$\alpha^9 = (1010)$	$\alpha^{10} = (0111)$
$\alpha^{11} = (1110)$	$\alpha^{12} = (1111)$	$\alpha^{13} = (1101)$	$\alpha^{14} = (1001)$	$\alpha^{15} = (0001)$

Ejemplo 5.4 *Representación en base polinomial para* $GF(2^{163})$. La reducción polinomial está dada por:

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1.$$

En su formato binario [2], el polinomio $f(x)$ se representaría como:

(10010011000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000000000000000000001)

Como puede observarse, resulta más práctico en el caso de polinomios de tal tamaño, utilizar una representación hexadecimal en lugar de la binaria. El polinomio $f(x)$ quedaría representado entonces en hexadecimal como:

0x9c0000000000000000000000000000000000000008.

Por ejemplo, si

$$g_1 = 0x29210f7937abf5e534be88d9f3d317f37a62d2d82$$

y

$$g_2 = 0x84076be406817ce9b54a2221b106f3851a48a6381$$

algunas resultados de operaciones sobre $GF(2^{163})$ son los siguientes,

$$g_1 + g_2 = 0xad26649d312a890c81f4aaf842d5e476602a74e03,$$

$$g_1 * g_2 = 0x7431a5d1b4d530af1da33cd69062ee32891b74332,$$

$$g_1^{-1} = 0xca53d2a114d8482e082265df8488ecb45542ab3f7.$$

[2] Tomando primero los bits menos significativos

5.3.2. Representación en bases normales

Por otro lado, además de las bases de representación polinomial descritas, tenemos las bases normales. Una *base normal* de $GF(2^m)$ sobre $GF(2)$ es una base de la forma

$$\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\},$$

donde $\beta \in GF(2^m)$. Cualquier elemento $a \in GF(2^m)$ puede ser escrito como

$$a = \sum_{i=0}^{m-1} a_i \beta^{2^i},$$

donde $a_i \in \{0, 1\}$. Las bases normales existen para toda $n \geq 1$ [58]. La representación en bases normales tiene la ventaja de que elevar un elemento al cuadrado puede hacerse de manera muy eficiente. La multiplicación de elementos puede ser, sin embargo, complicada. Las bases normales son útiles principalmente en implementaciones de hardware, como en el caso de los *multiplicadores bit-seriales* descritos en [75].

Una medida de la complejidad del hardware de tales multiplicadores está dada por el número C_α de unos en la matriz binaria $T = (T_{ij})$ de tamaño $m \times m$ definida por

$$\alpha^{1+2^i} = \sum_{j=0}^{n-1} T_{ij} \alpha^{2^j}, \tag{5.1}$$

para $0 \leq i \leq n-1$. La matriz T determina completamente la estructura de la multiplicación para la base normal. Es claro que $C_\alpha \leq n^2$. Por otro lado, C_α satisface la cota inferior $C_\alpha \geq 2n - 1$ [71]. Cuando se alcanza la cota inferior, se dice que α genera una *base normal óptima* (BNO).

Bases normales óptimas Lo elementos de $GF(2^m)$ pueden ser representados usando una representación en bases normales óptimas, tal como se describe en esta sección. Las bases normales óptimas (BNO) existen solo para ciertos valores de m (ver [71]). En particular, una BNO de $GF(2^m)$ existe si y solo si se cumple una de las siguientes condiciones:

1. $m+1$ es primo, y 2 es primitivo en $GF(2^{m+1})$, en tal caso las n raices $(n+1)$-ésimas no triviales de la unidad forman una BNO para $GF(2^m)$ denominada una *BNO de tipo I*.

2. $2m+1$ es primo, y se cumple que 2 es primitivo en $GF(2^{m+1})$ o que $2m+1 \equiv 3 \pmod 4$ y el orden multiplicativo de 2 en $GF(2^{m+1})$ es

m, entonces $\alpha = \gamma + \gamma^{-1}$ genera una BNO de $GF(2^m)$, donde γ es una $(2m+1)$-ésima raiz de la unidad. Esta es denominada una *BNO de tipo II*.

Un elemento $a \in GF(2^m)$ se representa por la cadena binaria $a = (a_0 a_1 a_2 \cdots a_{m-1})$. La identidad multiplicativa está representada por la cadena de solamente unos, mientras que el elemento cero es la cadena binaria formada únicamente por ceros. La adición de elementos se hace mediante el XOR de sus representaciones binarias correspondientes.

En la siguiente discusión un polinomio $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1 x + a_0$, donde cada a_i pertenece al campo binario $GF(2)$, estará representado por la cadena binaria $a_{m-1}a_{m-2}\cdots a_1 a_0$ de longitud m. En forma equivalente la cadena binaria puede ser vista como un vector binario de longitud m.

Para llevar a cabo la multiplicación utilizando representación en bases normales óptimas hay que efectuar lo siguiente:

1. Si $GF(2^m)$ tiene una BNO tipo I entonces sea $f(x) = x^m + x^{m-1} + \cdots + x^2 + x + 1$. De otra forma, si $GF(2^m)$ tiene una BNO tipo II entonces se calcula $f(x) = f_m(x)$ usando la siguiente fórmula recursiva:

$$\begin{aligned} f_0(x) &= 1, \\ f_1(x) &= x + 1, \\ f_{i+1}(x) &= x f_i(x) + f_{i-1}(x),\ i \geq 1. \end{aligned}$$

   Tenemos que $f(x)$ es un polinomio de grado m con coeficientes en $GF(2)$. El conjunto de polinomios $\{x, x^2, x^{2^2}, \ldots, x^{2^{m-1}}\}$ módulo $f(x)$ forman una base de $GF(2^m)$ denominada *base normal*.

2. Se construye la matríz A de tamaño $m \times m$ cuya i-ésima fila, $0 \leq i \leq m-1$, es el vector binario correspondiente al polinomio x^{2^i} mód $f(x)$.

3. Se determina la matríz inversa de A, A^{-1}.

4. Se construye la matríz T de tamaño $m \times m$ cuya i-ésima fila, $0 \leq i \leq m-1$, se obtiene de la manera siguiente. Se calcula el polinomio $x \cdot x^{2^i}$ mód $f(x)$ y denótese al correspondiente vector binario como v. Entonces la i-ésima fila de T es el vector binario $v \cdot A^{-1}$.

5. Se determinan los coeficientes λ_{ij} como $\lambda_{ij} = T(j-i, -i)$, donde los índices de T se toman módulo m. Se da el caso de que $\lambda_{0j} = 1$ para precisamente una sola j, $0 \leq j \leq m-1$. También ocurre que para

cada i, $0 \leq i \leq m-1$, $\lambda_{ij} = 1$ para precisamente dos diferentes j, $0 \leq j \leq m-1$. De aqui que exactamente $2m-1$ de los m^2 coeficientes de la matríz T son 1 y el resto son 0.[3]

Sean $a = (a_0 a_1 a_2 \cdots a_{m-1})$ y $b = (b_0 b_1 b_2 \cdots b_{m-1})$ dos elementos en $GF(2^m)$. Entonces el producto de a y b es el elemento $c = (c_0 c_1 c_2 \cdots c_{m-1})$, donde los coeficientes c_k se calculan de acuerdo a la expresión:

$$c_k = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_{i+k} b_{j+k} \lambda_{ij}, \tag{5.2}$$

para $0 \leq k \leq m-1$, donde todos los subíndices son calculados módulo m.

Ejemplo 5.5 *Representación en bases normales óptimas para* $GF(2^4)$ Como se vió en el ejemplo 2, los elementos de $GF(2^4)$ son el conjunto de todas la 4-tuplas binarias

(0000)	(0001)	(0010)	(0011)	(0100)	(0101)	(0110)	(0111)
(1000)	(1001)	(1010)	(1011)	(1100)	(1101)	(1110)	(1111)

Para realizar la multiplicación de elementos tenemos:

1. $f(x) = x^4 + x^3 + x^2 + x + 1$.
2. La matríz A resulta ser:
$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$
3. La inversa de A es:
$$A^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$
4. La matríz T es calculada como:
$$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

[3]Es debido a esta razón que la base normal es denominada *base normal óptima*.

5. Los términos λ_{ij} con valor de 1 son: $\lambda_{0,2}$, $\lambda_{1,2}$, $\lambda_{1,3}$, $\lambda_{2,0}$, $\lambda_{2,1}$, $\lambda_{3,1}$ y $\lambda_{3,3}$.

Por lo tanto la multiplicación queda definida como $(a_0a_1a_2a_3)\cdot(b_0b_1b_2b_3) = (c_0c_1c_2c_3)$, donde

$$\begin{aligned} c_0 &= a_0b_2 + a_1(b_2+b_3) + a_2(b_0+b_1) + a_3(b_1+b_3) \\ c_1 &= a_1b_3 + a_2(b_3+b_0) + a_3(b_1+b_2) + a_0(b_2+b_0) \\ c_2 &= a_2b_0 + a_3(b_0+b_1) + a_0(b_2+b_3) + a_1(b_3+b_1) \\ c_3 &= a_3b_1 + a_0(b_1+b_2) + a_1(b_3+b_0) + a_2(b_0+b_2). \end{aligned}$$

Entre las observaciones que podemos hacer están las siguientes:

1. La identidad multiplicativa es (1111).

2. Puede comprobarse que

$$\begin{aligned} (a_0a_1a_2a_3)\cdot(a_0a_1a_2a_3) &= (a_0a_1a_2a_3)^2 \\ &= (a_3a_0a_1a_2), \end{aligned}$$

   de manera que el elevar al cuadrado un elemento del campo se reduce a un desplazamiento cíclico a la derecha de su representación vectorial.

Bases normales Gaussianas El estándar ANSI X.96 [4] recomienda el uso de las *bases normales Gaussianas*. Definiremos a continuación el concepto de bases normales Gaussianas.

Sea q un primo o la potencia de un primo, y sean N,t enteros positivos tales que $(Nt+1)$ es un primo que no divide a q. Sea τ una raíz t-ésima primitiva de la unidad en $\mathbb{Z}/(Nt+1)\mathbb{Z}$. Sea γ una raíz $(Nt+1)$-ésima de la unidad en el campo $GF(q)$. Un *periodo de Gauss* de tipo (N,t) sobre $GF(q)$ se define [63] como

$$\alpha = \sum_{i=0}^{t-1} \gamma^{\tau^i}.$$

La base normal generada por el periodo de Gauss de tipo (N,t) es denominada una base normal Gaussiana de tipo t [63].

Una base normal Gaussiana (BNG) existe siempre que m no sea divisible por 8. Sea m un entero positivo no divisible por 8, y sea T un entero positivo. Entonces una BNG de tipo T para $GF(2^m)$ existe si y solo si $p = Tm+1$ es primo y $MCD(Tm/k, m) = 1$, donde k es el orden multiplicativo de 2 mod

p. Dadas m y T, el campo $GF(2^m)$ tiene a lo más una BNG de tipo T [71] [6].

Si $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}$ es una base normal de $GF(2^m)$ sobre $GF(2)$, entonces el elemento $a = \sum_{i=0}^{m-1} a_i \beta^{2^i}$ del campo está representado por la cadena binaria $(a_0 a_1 \cdots a_{m-1})$ de longitud m, de modo que:

$$GF(2^m) = \{(a_0 a_1 \cdots a_{m-2} a_{m-1}) \ : \ a_i \in \{0,1\}\}.$$

Se define entonces las siguientes operaciones aritméticas sobre los elementos de $GF(2^m)$ cuando se utiliza una BNG de tipo T:

- Adición: Si $(a_0 a_1 \cdots a_{m-2} a_{m-1})$ y $(b_0 b_1 \cdots b_{m-2} b_{m-1})$ son elementos de $GF(2^m)$, entonces $a + b = c = (c_0 c_1 \cdots c_{m-2} c_{m-1})$ donde $c_i = a_i + b_i \bmod 2$.

- Cuadrado: Sea $(a_0 a_1 \cdots a_{m-2} a_{m-1}) \in GF(2^m)$. Entonces,

  $$a^2 = \left(\sum_{i=0}^{m-1} a_i \beta^{2^i} \right)^2 = \sum_{i=0}^{m-1} a_i \beta^{2^{i+1}} = \sum_{i=0}^{m-1} a_{i-1} \beta^{2^i},$$

  y por lo tanto $a^2 = (a_{m-1} a_0 a_1 \cdots a_{m-2})$, esto es, para elevar al cuadrado basta hacer una simple rotación de la representación vectorial.

- Multiplicación: Sean $p = Tm + 1$ y $u \in GF(2^m)$ un elemento de orden T. Definamos la secuencia $F(1), F(2), \ldots, F(p-1)$ como

  $$F(2^i u^j \bmod p) = i$$

  para $0 \leq i \leq m-1, 0 \leq j \leq T-1$. Si $(a_0 a_1 \cdots a_{m-2} a_{m-1})$ y $(b_0 b_1 \cdots b_{m-1} b_{m-2})$ son elementos de $GF(2^m)$, entonces $a \cdot b = c = (c_0 c_1 \cdots c_{m-2} c_{m-1})$ donde

  $$c_l = \sum_{k=1}^{p-1} a_{F(k+1)+l} b_{F(p-k)+l}$$

  si T es par, y

  $$\begin{aligned} c_l &= \sum_{k=1}^{m/2} (a_{k+l-1} b_{m/2+k+l-1} + a_{m/2+k+l-1} b_{k+l-1}) \\ &+ \sum_{k=1}^{p-2} a_{F(k+1)+l} b_{F(p-k)+l} \end{aligned}$$

  si T es impar, para $0 \leq l \leq m-1$.

- Inversión: Si a es un elemento de $GF(2^m)$ diferente de cero, el *inverso* de a, denotado por a^{-1}, es el elemento $c \in GF(2^m)$ tal que $c \cdot a = 1$.

Ejemplo 5.6 *Representación en bases normales Gaussianas para* $GF(2^4)$ Consideremos la BNG de tipo $T = 3$ para $GF(2^4)$. El elemento $u = 9 \in GF(13)$ es de orden 3. La secuencia $F(i)$ es:

$$\begin{array}{llllll} F(1) = 0 & F(2) = 1 & F(3) = 0 & F(4) = 2 & F(5) = 1 & F(6) = 1 \\ F(7) = 3 & F(8) = 3 & F(9) = 0 & F(10) = 2 & F(11) = 3 & F(12) = 2. \end{array}$$

Las fórmulas para los términos c_l del producto son:

$$\begin{aligned} c_0 &= a_0(b_1 + b_2 + b_3) + a_1(b_0 + b_2) + a_2(b_0 + b_1) + a_3(b_0 + b_3) \\ c_1 &= a_1(b_2 + b_3 + b_0) + a_2(b_1 + b_3) + a_3(b_1 + b_2) + a_0(b_1 + b_0) \\ c_2 &= a_2(b_3 + b_0 + b_1) + a_3(b_2 + b_0) + a_0(b_2 + b_3) + a_1(b_2 + b_1) \\ c_3 &= a_3(b_0 + b_1 + b_2) + a_0(b_3 + b_1) + a_1(b_3 + b_0) + a_2(b_3 + b_2). \end{aligned}$$

Por ejemplo, si $a = (1000)$ y $b = (1101)$, entonces $c = a \cdot b = (0010)$.