ARREGLOS COSTAS

YULY PAOLA DORADO YACUMAL
FERNANDO MUÑOZ PAZ

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN, CAUCA
2012

ARREGLOS COSTAS

TRABAJO DE GRADO

En la modalidad de Seminario de Grado presentado

como requisito parcial para optar al título de Matemático

YULY PAOLA DORADO YACUMAL

FERNANDO MUÑOZ PAZ

Director:

Dr. CARLOS ALBERTO TRUJILLO SOLARTE

UNIVERSIDAD DEL CAUCA

FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN

DEPARTAMENTO DE MATEMÁTICAS

POPAYÁN, CAUCA

2012

Nota de aceptación _____

_____

_____

_____

Director:

_____

Dr. Carlos Alberto Trujillo Solarte

Jurados:

_____

Profesor. Alfredo Gomez Calvache

_____

Profesor. Diego Fernando Ruiz Solarte

Fecha de sustentación: Popayán, Mayo 3 de 2012

Este trabajo está dedicado a mi madre Cecilia Yacumal, a mis padres Olmedo Dorado y Jorge Contreras, a mis hermanos John, Daniela y Stefany. A mis abuelos Teresa, Bertilde y Rosaliano (QDEP) , a mis tios y tias Laurentino, Alfonso, Virginia, Susana y Mercedes, a mis primas Viviana, Salma y Sinthia. A Nelson. Y demás familiares.

A mis padres Gildardo Muñoz y Consuelo Paz, a mi esposa Yuly Viviana Cruz, a mis hijos Yuliet Katerine y Luis Fernando.

Agradecimientos

Agradecemos a Dios por darnos la oportunidad de culminar un sueño más en nuestras vidas y de haber tenido el privilegio de contar con la valiosa, paciente e innegable colaboración del Dr. Carlos Alberto Trujillo Solarte, director de este trabajo quien no sólo compartió con nosotros sus conocimientos sino que nos instruyó e inspiro para ser mejores personas y buenos profesionales.

A los profesores Diego Fernando Ruiz Solarte y Alfredo Gomez Calvache miembros del comité de seguimiento por todas sus sugerencias y aportes.

A la Universidad del Cauca y a todos los profesores que estuvieron en este proceso de formación profesional.

A nuestras familias por el apoyo incondicional que siempre nos han brindado.

A nuestros amigos y compañeros que durante estos años estuvieron a nuestro lado brindándonos todo su apoyo y a todas aquellas personas que de una u otra forma colaboraron o participaron en la realización del presente trabajo.

Introducción

Los arreglos Costas son un tema moderno que ha llamado la atención de la comunidad matemática y en especial la nuestra, pues sólo desde el año 1960 el Dr. Jhon Costas motivado por una aplicación al radar y al sonar empieza explorando las matrices y sus permutaciones, y encuentra ejemplos de tales arreglos hasta tamaño $n = 12$. Debido a que encuentra dificultades para la construcción de arreglos $n \geq 12$, recibe la ayuda del profesor Solomon Golomb (matemático) quien con técnicas basadas en la teoría de campos finitos le permite construir estos arreglos.

En [2] se presenta una tabla con el número exacto de arreglos Costas hasta orden $n = 27$. En el año 2011 con la ayuda de técnicas computacionales ya se tiene el número exacto de arreglos Costas para $n = 28$ y $n = 29$; aunque no se tenga el número exacto de arreglos Costas para orden $n = 30$ y $n = 31$ se sabe que sí existen dichas construcciones, lo curioso es que para $n = 32$ y $n = 33$ aún no se han encontrado ejemplos de dichos arreglos, dando lugar a las preguntas ¿existen estos arreglos?, ¿existen arreglos para todo n?

Este trabajo no pretende responder a estos interrogantes pero si estudiar y analizar los arreglos Costas, sus construcciones y relaciones, basados en el artículo "The Status of Costas Arrays" del profesor Solomon Golomb ([2]) y crear un referente para trabajos posteriores.

Este documento está organizado de la siguiente manera. El Capítulo 1 contiene las diferentes definiciones y notaciones de los arreglos Costas, y sus construcciones. En el Capítulo 2 se hace una analogía del primer capitulo pero teniendo en cuenta los conjuntos de Si-

don. El Capítulo 3 analiza la construcción de Welch con mas detalle. En el Apéndice A se presentan algunos resultados necesarios de la Teoría de Campos Finitos. El Apéndice B expone un listado de las construcciones tipo Welch y tipo Golomb. En el Apéndice C se muestra una tabla con el número exacto de arreglos Costas hasta orden 29, y sus rotaciones, reflexiones y simetrías.

Índice general

Índice de tablas

Índice de figuras

Capítulo 1

Arreglos Costas Clásicos

En este capítulo se presentan los conceptos, la notación y las construcciones de los arreglos Costas.

1.1. Conceptos, Notación Y Ejemplos

De fofrma usual se definen:
Sea $n \in \mathbb{Z}^+$, $[1,n] := \{1,2,\ldots,n\}$, $[1,n]^2 := [1,n] \times [1,n]$, y
$[1,n]^2 := \{(i,j) \in \mathbb{Z} \times \mathbb{Z} : 1 \leq i,j \leq n\}$.

Definición 1.1.1. *Un* **arreglo Costas** *de orden n es un subconjunto C de $[1,n]^2$ tal que ningún par de puntos en C está en la misma fila o en la misma columna, y tal que ningún par de los $\binom{n}{2}$ segmentos de recta entre pares de puntos en C son iguales en magnitud y pendiente, es decir, es libre de paralelogramos.*

Algunas definiciones equivalentes de arreglos Costas se muestran a continuación:

Definición 1.1.2. *Un arreglo cuadrado $n \times n$ de puntos y blancos es un arreglo Costas si satisface:*

1. *Existen n puntos, uno en cada fila y uno en cada columna del arreglo.*
2. *Los $\binom{n}{2}$ segmentos de recta entre pares de puntos difieren en magnitud o pendiente.*

Definición 1.1.3. *Sea $C = (C_{ij})_{n\times n}$ una matriz cuadrada de orden n, con $c_{ij} \in \{0,1\}$. C es un arreglo Costas de orden n si*

1. *Existe un único $c_{ij} = 1$ en cada fila y columna.*
2. *Los $\binom{n}{2}$ segmentos de recta entre pares de puntos correspondientes a 1's son distintos.*

   Es decir dados $c_{i_1j_1} = c_{i_2j_2} = c_{i_3j_3} = c_{i_4j_4} = 1$ en C se debe cumplir que
   $(i_2 - i_1, j_2 - j_1) \neq (i_4 - i_3, j_4 - j_3)$ *y* $(i_2 - i_1, j_2 - j_1) \neq (i_3 - i_2, j_3 - j_2)$.

Nota 1.1.1. Los 1's son las coordenadas dadas, convencionalmente la primera coordenada se ubicará horizontalmente de izquierda a derecha y la segunda coordenada se ubicará verticalmente de abajo hacia arriba.

Comentario 1.1.1. Si $C \subseteq [1,n]^2$ es un arreglo Costas de orden n, éste puede verse como una permutación de $[1,n]$

$$\begin{aligned} C : [1,n] &\rightarrow [1,n] \\ i &\longmapsto c(i) \end{aligned}$$

con $c(i) = j$. Así, $C = \{(1,c(1)),(2,c(2)),...,(n,c(n))\}$, donde $[c(1),c(2),...,c(n)]$, es llamado **vector permutación**.

Observación 1.1.1. Un arreglo Costas es un conjunto de diferencias distintas, ya que si dadas $(i,c_i),(j,c_j)$ y $(k,c_k),(l,c_l)$ en las que la primera componente son iguales entonces $c_i - c_j \neq c_k - c_l$, $\forall i \neq k$ y $\forall j \neq l$. Esto se ilustra en la Tabla 1.1.

Observe que en cada diagonal (no principal) las segundas componentes son distintas, de donde el arreglo formado por las segundas componentes de dichas diagonales se llama **triángulo de diferencias** asociado al conjunto C y la representación se muestra en la Tabla 1.2.

$(1,\, c_1)$	$(2,\, c_2)$	$(3,\, c_3)$	$(4,\, c_4)$	...	$(i,\, c_i)$	...	$(n,\, c_n)$
$(0,\, 0)$	$(1,\, c_2 - c_1)$	$(2,\, c_3 - c_1)$	$(3,\, c_4 - c_1)$	...	$(i-1,\, c_i - c_1)$	...	$(n-1,\, c_n - c_1)$
	$(0,\, 0)$	$(1,\, c_3 - c_2)$	$(2,\, c_4 - c_2)$	...	$(i-2,\, c_i - c_2)$	...	$(n-2,\, c_n - c_2)$
		$(0,\, 0)$	$(1,\, c_4 - c_3)$	...	$(i-3,\, c_i - c_3)$	...	$(n-3,\, c_n - c_3)$
			$(0,\, 0)$	...	$(i-4,\, c_i - c_4)$	...	$(n-4,\, c_n - c_4)$
				...	... ...	...	... ...
					$(1,\, c_i - c_{i-1})$	...	$(2,\, c_n - c_{n-2})$
					$(0,0)$	...	$(1, c_n - c_{n-1})$
							$(0,0)$

Tabla 1.1: Diferencias distintas asociado al conjunto $C = \{(1, c_1), (2, c_2), \cdots, (n, c_n)\}$

c_1	c_2	c_3	c_4	...	...	...	...	c_n
$c_2 - c_1$	$c_3 - c_2$	$c_4 - c_3$	$c_5 - c_4$	...	...	...	$c_n - c_{n-1}$	
	$c_3 - c_1$	$c_4 - c_2$	$c_5 - c_3$	...	...	$c_n - c_{n-2}$		
		$c_4 - c_1$	$c_5 - c_2$	...	...	$c_n - c_{n-3}$		
			...		...			
			$c_{n-1} - c_1$		$c_n - c_2$			
				$c_n - c_1$				

Tabla 1.2: Triángulo de diferencias asociado al conjunto $C = \{(1, c_1), (2, c_2), \cdots, (n, c_n)\}$

Ejemplo 1.1.1. *El conjunto* $C = \{(1,1), (2,3), (3,4), (4,2), (5,5)\}$ *notado respectivamente como* $C = \{C_1, C_2, C_3, C_4, C_5\}$ *es un arreglo Costas de orden 5, ya que los* $\binom{5}{2} = 10$ *segmentos de recta asociados con pares de puntos en* C *son distintos en magnitud y pendiente, como se verifica en la Tabla* 1.3.

De otro lado, en las Figuras 1.1 *y* 1.2 *se observa la representación gráfica del conjunto* C*, donde se ve que está libre de paralelogramos. Note que los vectores que tienen igual magnitud tienen distinta pendiente y viceversa.*

	Magnitud	Pendiente
$\overrightarrow{C_1C_2}$	$\sqrt{5}$	2
$\overrightarrow{C_1C_3}$	$\sqrt{13}$	$\frac{3}{2}$
$\overrightarrow{C_1C_4}$	$\sqrt{10}$	$\frac{1}{3}$
$\overrightarrow{C_1C_5}$	$\sqrt{32}$	1
$\overrightarrow{C_2C_3}$	$\sqrt{2}$	1
$\overrightarrow{C_2C_4}$	$\sqrt{5}$	$-\frac{1}{2}$
$\overrightarrow{C_2C_5}$	$\sqrt{13}$	$\frac{2}{3}$
$\overrightarrow{C_3C_4}$	$\sqrt{5}$	-2
$\overrightarrow{C_3C_5}$	$\sqrt{5}$	$\frac{1}{2}$
$\overrightarrow{C_4C_5}$	$\sqrt{10}$	3

Tabla 1.3: Comparación magnitud y pendiente de todos los pares de puntos del conjunto $C = \{(1,1),(2,3),(3,4),(4,2),(5,5)\}$

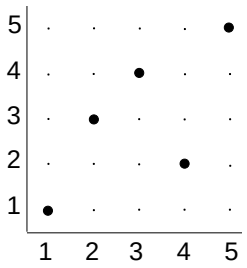


Figura 1.1: Representación gráfica del conjunto $C = \{(1,1),(2,3),(3,4),(4,2),(5,5)\}$

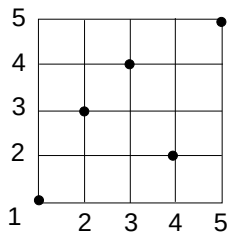


Figura 1.2: Representación gráfica del conjunto $C = \{(1,1),(2,3),(3,4),(4,2),(5,5)\}$

Ahora, tomando las $\binom{5}{4} = 5$ *posibilidades se tiene:*

1. $c_{11} = c_{23} = c_{34} = c_{42} = 1$

$(2-1,3-1) \neq (4-3,2-4)$ y $(2-1,3-1) \neq (3-2,4-3)$

$(1,2) \neq (1,-2)$ y $(1,2) \neq (1,1)$

2. $c_{23} = c_{34} = c_{42} = c_{55} = 1$

   $(3-2,4-3) \neq (5-4,5-2)$ y $(3-2,4-3) \neq (4-3,2-4)$

   $(1,1) \neq (1,3)$ y $(1,1) \neq (1,-2)$

3. $c_{11} = c_{34} = c_{42} = c_{55} = 1$

   $(3-1,4-1) \neq (5-4,5-2)$ y $(3-1,4-1) \neq (4-3,2-4)$

   $(2,3) \neq (1,3)$ y $(2,3) \neq (1,-2)$

4. $c_{11} = c_{23} = c_{42} = c_{55} = 1$

   $(2-1,3-1) \neq (5-4,5-2)$ y $(2-1,3-1) \neq (4-2,2-3)$

   $(1,2) \neq (1,3)$ y $(1,2) \neq (2,-1)$

5. $c_{11} = c_{23} = c_{34} = c_{55} = 1$

   $(2-1,3-1) \neq (5-3,5-4)$ y $(2-1,3-1) \neq (3-2,4-3)$

   $(1,2) \neq (2,1)$ y $(1,2) \neq (1,1)$.

Note que la representación del arreglo Costas C aplicando la Definición 1.1.3, *se da mediante la matriz*

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

de donde el vector permutación asociado a C es $[1,3,4,2,5]$.

El conjunto de diferencias distintas y el triángulo de diferencias asociado a C se representan en las Tablas 1.4 *y* 1.5

$(1,\ 1)$	$(2,\ 3)$	$(3,\ 4)$	$(4,\ 2)$	$(5,\ 5)$
$(0,\ 0)$	$(1,\ 2)$	$(2,\ 3)$	$(3,\ 1)$	$(4,\ 4)$
	$(0,\ 0)$	$(1,\ 1)$	$(2,-1)$	$(3,\ 2)$
		$(0,0)$	$(1,-2)$	$(2,\ 1)$
			$(0,\ 0)$	$(1,\ 3)$
				$(0,\ 0)$

Tabla 1.4: Conjunto de diferencias distintas de $C = \{(1,1),(2,3),(3,4),(4,2),(5,5)\}$

1	3	4	2	5
2	1	-2	3	
3	-1	1		
1	2			
4				

Tabla 1.5: Triángulo de diferencias de la permutación $C = [1,3,4,2,5]$.

Ejemplo 1.1.2. *El conjunto* $C = \{(1,1),(2,2),(3,4),(4,3),(5,5)\}$ *notado ordenadamente como* $C = \{C_1, C_2, C_3, C_4, C_5\}$ *no es un arreglo Costas de orden* 5.
Aplicando la Definición 1.1.2

	Magnitud	Pendiente
$\overrightarrow{C_2C_3}$	$\sqrt{5}$	2
$\overrightarrow{C_2C_4}$	$\sqrt{5}$	$\frac{1}{2}$
$\overrightarrow{C_3C_5}$	$\sqrt{5}$	$\frac{1}{2}$
$\overrightarrow{C_4C_5}$	$\sqrt{5}$	2

Tabla 1.6: Comparación magnitud y pendiente relacionada al conjunto $C = \{(1,1),(2,2),(3,4),(4,3),(5,5)\}$

En la Tabla 1.6 *se observa que los vectores formados por los puntos* C_2, C_3 *y* C_4, C_5 *tienen igual magnitud y pendiente, de la misma manera que los vectores formados por los puntos* C_2, C_4 *y* C_3, C_5.
Observe la formación del paralelogramo. Aplicando la definición 1.1.3

- Si $c_{22} = c_{34} = c_{43} = c_{55} = 1$ entonces $(3-2, 4-2) = (5-4, 5-3)$, es decir $(1,1) = (1,1)$.

Luego no cumple la Definición 1.1.3.

Note que la permutación asociada a C *es* $[1,2,4,3,5]$.

El conjunto de diferencias distintas y el triángulo de diferencias asociados a C *se representan en las Tablas* 1.7 *y* 1.8. *Se observa que hay diferencias iguales.*

$(1,\ 1)$	$(2,\ 2)$	$(3,\ 4)$	$(4,\ 3)$	$(5,\ 5)$
$(0,\ 0)$	$(1,\ 1)$	$(2,\ 3)$	$(3,\ 2)$	$(4,\ 4)$
	$(0,\ 0)$	$\underline{(1,\ 2)}$	$\underline{(2,\ 1)}$	$(3,\ 3)$
		$(0,0)$	$(1,-1)$	$\underline{(2,\ 1)}$
			$(0,\ 0)$	$\underline{(1,\ 2)}$
				$(0,\ 0)$

Tabla 1.7: Diferencias distintas de $C = [1,2,4,3,5]$.

1	2	4	3	5
1	$\underline{2}$	-1	$\underline{2}$	
3	$\underline{1}$	$\underline{1}$		
2	3			
4				

Tabla 1.8: Triángulo de diferencias de $C = [1,2,4,3,5]$.

1.2. Construcciones Conocidas

En esta sección se presentan las construcciones de arreglos Costas conocidas, las cuales involucran el uso de raíces primitivas en campos finitos. Para sus demostraciones se usará la siguiente nota.

Nota 1.2.1. Considere el conjunto $C = \{(1, c(1)), (2, c(2)), \ldots, (n, c(n))\}$ de puntos en el retículo $[1,n] \times [1,n]$. Para demostrar que C es un arreglo Costas se debe probar lo siguiente:

1. $[c(1), c(2), ..., c(n)]$ es una permutación de $[1, n]$.

2. No existen dos pares de puntos

$$\{(i, c(i)), (i+k, c(i+k))\}$$

$$\{(l, c(l)), (l+k, c(l+k))\}$$

con $i \neq l$, cuyos vectores diferencia $(k, c(i+k)) - c(i))$ y $(k, c(l+k)) - c(l))$ sean iguales. Es decir, no es posible tener que

$$c(i+k) - c(i) = c(l+k) - c(l)$$

para i, k, l tales que $1 \leq i < i+k \leq n$ y $1 \leq l < l+k \leq n$.

1.2.1. Construcción De Welch

Sean p un número primo y g una raíz primitiva módulo p.

Teorema 1.2.1. *La matriz permutación $W = (w_{ij})$ de orden $(p-1) \times (p-1)$, donde*

$$w_{ij} = 1 \Leftrightarrow j \equiv g^i \pmod{p}, \quad 1 \leq i, j \leq p-1$$

es un arreglo Costas. Es decir el conjunto $W = \{(i, g^i \pmod{p}) : 1 \leq i \leq p-1\}$, es un arreglo Costas de orden $p-1$.

Demostración. Como g es una raíz primitiva módulo p, entonces $[g^1, g^2, ..., g^{p-1}]$ es una permutación de $[1, p-1]$, con lo que la Condición 1 de la Nota 1.2.1 se satisface. Resta probar que los $\binom{p-1}{2}$ vectores diferencia son distintos. Para ello suponga que existen dos pares de puntos

$$\left\{(i, g^i \pmod{p}), (i+k, g^{i+k} \pmod{p})\right\}$$

$$\left\{(l, g^l \pmod{p}), (l+k, g^{l+k} \pmod{p})\right\},$$

con $i \neq l$, $1 \leq i < i+k \leq p-1$ y $1 \leq l < l+k \leq p-1$, tal que los vectores diferencia son iguales. Es decir $(k, (g^{i+k} - g^i) \pmod{p}) = (k, (g^{l+k} - g^l) \pmod{p})$, de donde

$$g^{i+k} - g^i \equiv g^{l+k} - g^l \pmod{p}$$

$$g^i(g^k - 1) \equiv g^l(g^k - 1) \pmod{p}$$

ya que $1 < k < p-1$, entonces $g^k - 1 \not\equiv 0 \pmod{p}$, y así se sigue que $g^i \equiv g^l \pmod{p}$, con lo que

$$i \equiv l \pmod{p-1}$$

y como $1 < i, l < p-1$, se tiene que $i = l$. □

Ejemplo 1.2.1. *Sean $p = 11$, $g = 2$. Aplicando la construcción de Welch se obtiene que $W = \{(1,2),(2,4),(3,8),(4,5),(5,10),(6,9),(7,7),(8,3),(9,6),(10,1)\}$ es un arreglo Costas tipo Welch de orden 10.*

En la Figura 1.5 *se ilustra el comportamiento de los elementos de W en el retículo $[1,10]\times[1,10]$, donde se observa que en cada fila y en cada columna hay un sólo elemento, y que además ningún cuatro de ellos forma un paralelogramo.*

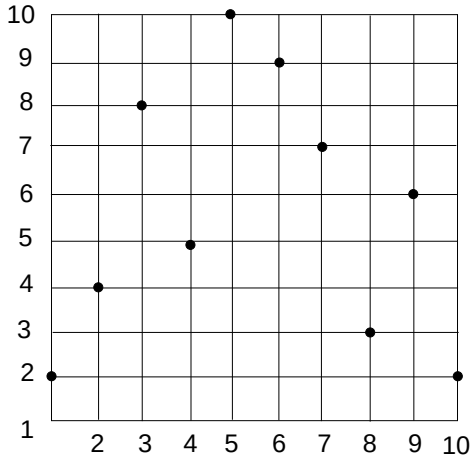


Figura 1.3: Ilustración gráfica del arreglo Costas tipo Welch en el retículo $[1,10]\times[1,10]$.

Nota 1.2.2. En adelante se usará únicamente la representación gráfica asociada a la Definición 1.1.2.

1.2.2. Construcción De Lempel

Sea q una potencia de un número primo y $\mathbb{F}_q$ el único campo finito con q elementos (salvo isomorfismos). Observe que si α es un generador de $\mathbb{F}_q^*$, entonces

$$\begin{aligned}\mathbb{F}_q^* &= \langle\alpha\rangle \\ &:= \left\{\alpha^1, \alpha^2, ..., \alpha^{q-2}, \alpha^{q-1} = 1\right\} \\ &= \left\{\alpha^i : 1 \leq i \leq q-1\right\}, \alpha^i \neq 0.\end{aligned}$$

Teorema 1.2.2. *Para todo $q > 2$ y α generador de $\mathbb{F}_q^*$, el conjunto:*

$$L := \left\{(i,j) : \alpha^i + \alpha^j = 1, 1 \leq i, j \leq q-2\right\}$$

es un arreglo Costas de orden $q-2$.

Demostración. Observe que $\alpha^i + \alpha^j = 1$ equivale a $j = \log_\alpha(1-\alpha^i)(\mod q)$ con lo que $i, j \neq q-1$ ($\alpha^i = 1 \Leftrightarrow i = q-1$).
Por lo tanto

$$L = \left\{(i, \log_\alpha(1-\alpha^i) \pmod q) : 1 \leq i \leq q-2\right\}.$$

Es claro además que $\{\log_\alpha(1-\alpha^i) : 1 \leq i \leq q-2\} = \{1, 2, 3, ..., q-2\}$, con lo que la condición 1 de la Nota 1.2.1 se satisface. Resta probar que los $\binom{q-2}{2}$ vectores diferencia son distintos. Para ello suponga que existen dos pares de puntos

$$\left\{(i, \log_\alpha(1-\alpha^i)), (i+k, \log_\alpha(1-\alpha^{i+k}))\right\}$$

$$\left\{(l, \log_\alpha(1-\alpha^l)), (l+k, \log_\alpha(1-\alpha^{l+k}))\right\}$$

con $i \neq l$, $1 \leq i < i+k \leq q-2$ y $1 \leq l < l+k \leq q-2$, tal que los vectores diferencia son iguales. Es decir

$$(k, \log_\alpha(1-\alpha^i) - \log_\alpha(1-\alpha^{i+k})) = (k, \log_\alpha(1-\alpha^l) - \log_\alpha(1-\alpha^{l+k}))$$

de donde

$$\log_\alpha((1-\alpha^i)(1-\alpha^{l+k})) = \log_\alpha((1-\alpha^l)(1-\alpha^{i+k}))$$

$$(1-\alpha^i)(1-\alpha^{l+k}) = (1-\alpha^l)(1-\alpha^{i+k})$$

$$\alpha^i + \alpha^{l+k} = \alpha^l + \alpha^{i+k}$$

$$\alpha^k(\alpha^l - \alpha^i) = (\alpha^l - \alpha^i)$$

ya que $l \neq k$, y $\alpha^i \neq \alpha^l$, se tiene que $\alpha^k = 1$, lo cual no es posible porque $1 < k < q-2$. □

Ejemplo 1.2.2. *Los elementos primitivos de* $q = 11$ *son* $2, 6, 7$ *y* 8. *A continuación se aplicará la construcción de Lempel para* $\alpha = 2$. *Mediante la Tabla* 1.9 *se muestra la construcción del arreglo, de donde se tiene que*
$L = \{(1,5),(2,3),(3,2),(4,7),(5,1),(6,8),(7,4),(8,6),(9,9)\}$ *es un arreglo Costas tipo Lempel de tamaño* 9, *como se ilustra en la Figura* 1.4

i	1	2	3	4	5	6	7	8	9	10
$2^i \pmod{11}$	2	4	8	5	10	9	7	3	6	1
$(1-2^i) \pmod{11}$	10	8	4	7	2	3	5	9	6	–
$j = \log_2(1-2^i)$	5	3	2	7	1	8	4	6	9	−−

Tabla 1.9: Construcción de arreglo Costas tipo Lempel con $q = 11$ y $\alpha = 2$

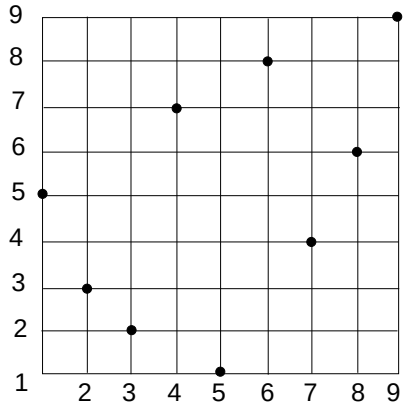


Figura 1.4: Arreglo Costas tipo Lempel en el retículo $[1,9] \times [1,9]$.

1.2.3. Construcción De Golomb

Sea q una potencia de un número primo, $\mathbb{F}_q$ el único campo finito con q elementos (salvo isomorfismos) y α, β elementos primitivos de $\mathbb{F}_q$ (es decir, generadores del grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$).

Teorema 1.2.3. *Para todo $q > 2$, el conjunto*

$$G := \left\{(i,j) : \alpha^i + \beta^j = 1, 1 \leq i, j \leq q-2\right\}$$

es un arreglo Costas de orden $q-2$.

Demostración. Note que la condición $\alpha^i + \beta^j = 1$ es equivalente a $j = \log_\beta(1-\alpha^i)$. Esto obliga a que i, j sean diferentes de $q-1$. Por lo tanto

$$G = \left\{(i, \log_\beta(1-\alpha^i)) : 1 \leq i \leq q-2\right\}$$

si y sólo si $\alpha^i = \alpha^j$ de donde $i = j$, ya que $\log_\beta(1-\alpha^i) = \log_\beta(1-\alpha^j), \quad 1 \leq i, j \leq q-2$. Entonces $\left\{\log_\beta(1-\alpha^i) : 1 \leq i \leq q-2\right\} = \{1, 2, 3, ..., q-2\}$ con lo que la Condición 1 de la Nota 1.2.1 se satisface. Resta probar que los $\binom{q-2}{2}$ vectores diferencia son distintos. Suponga que existen dos pares de puntos

$$\left\{(i, \log_\beta(1-\alpha^i)), (i+k, \log_\beta(1-\alpha^{i+k}))\right\}$$

$$\left\{(l, \log_\beta(1-\alpha^l)), (l+k, \log_\beta(1-\alpha^{l+k}))\right\}$$

con $i \neq l$, $1 \leq i < i+k \leq q-2$ y $1 \leq l < l+k \leq q-2$, tal que los vectores diferencia son iguales. Es decir

$$(k, \log_\beta(1-\alpha^i) - \log_\beta(1-\alpha^{i+k})) = (k, \log_\beta(1-\alpha^l) - \log_\beta(1-\alpha^{l+k}))$$

de donde

$$\log_\beta((1-\alpha^i)(1-\alpha^{l+k})) = \log_\beta((1-\alpha^l)(1-\alpha^{i+k}))$$

$$(1-\alpha^i)(1-\alpha^{l+k}) = (1-\alpha^l)(1-\alpha^{i+k})$$

$$\alpha^i + \alpha^{l+k} = \alpha^l + \alpha^{i+k}$$

$$\alpha^k(\alpha^l - \alpha^i) = \alpha^l - \alpha^i$$

ya que$l \neq i$, se tiene que $\alpha^k = 1$, lo cual no es posible porque $1 < k < q-2$. □

Ejemplo 1.2.3. *En la Tabla* 1.10 *se aplicará la construcción de Golomb para* $q = 11$, $\alpha = 2$, *y* $\beta = 8$.

i	1	2	3	4	5	6	7	8	9	10
$2^i(\text{mód}11)$	2	4	8	5	10	9	7	3	6	1
$8^i(\text{mód}11)$	8	9	6	4	10	3	2	5	7	1
$(1-2^i)(\text{mód}11)$	10	8	4	7	2	3	5	9	6	–
$j = \log_8(1-2^i)$	5	1	4	9	7	6	8	2	3	$--$

Tabla 1.10: Construcción de arreglo Costas tipo Golomb con $q = 11$, $\alpha = 2$, y $\beta = 8$.

de donde se obtiene $G = \{(1,5),(2,1),(3,4),(4,9),(5,7),(6,6),(7,8),(8,2),(9,3)\}$ *que es un arreglo Costas tipo Golomb de orden* 9.
La Figura 1.5 *muestra la distribución de los elementos de* G *en el retículo* $[1,9] \times [1,9]$.

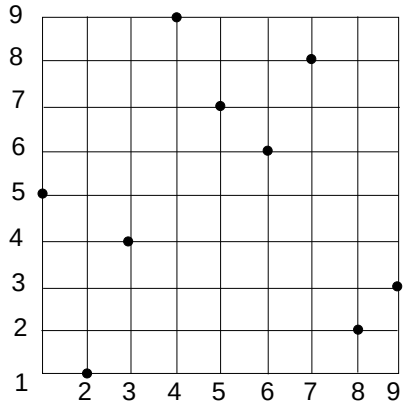


Figura 1.5: Arreglo Costas tipo Golomb en el retículo $[1,9] \times [1,9]$.

Note que la construcción de Lempel es un caso particular de la construcción de Golomb tomando $\alpha = \beta$.

1.3. Otras Construcciones

Lema 1.3.1. *Si un arreglo Costas* $n \times n$ *tiene un* 1 *en alguna de las cuatro esquinas, la correspondiente fila y columna pueden ser eliminadas, obteniendo un arreglo Costas de*

orden $(n-1)\times(n-1)$.

Demostración. Suponga que $C_n = \{(1,c(1)),(2,c(2)),\ldots,(n,c(n))\}$ es un arreglo Costas de tamaño $n \times n$.

- Si $(1,1) \in C$ entonces $c(1) = 1$, así

$$\begin{aligned} C_{n-1} &= \{(2,c(2)),(3,c(3)),...,(n,c(n))\} - (1,1) \\ &= \{(1,c(2)-1),(2,c(3)-1),...,(n-1,c(n)-1)\} \end{aligned}$$

  con lo que el vector permutación $[c(2)-1, c(3)-1, ..., c(n)-1]$ determina el nuevo arreglo Costas.

- Si $(n,1) \in C$ entonces $c(n) = 1$, así

$$\begin{aligned} C_{n-1} &= \{(1,c(1)),(2,c(2)),...,(n,c(n))\} - (n,1) \\ &= \{(1,c(1)-1),(2,c(2)-1),...,(n-1,c(n)-1)\} \end{aligned}$$

  con lo que el vector permutación $[c(1)-1, c(2)-1, ..., c(n)-1]$ determina el nuevo arreglo Costas.

- Si $(1,n) \in C$ entonces $c(n) = 1$, así

$$\begin{aligned} C_{n-1} &= \{(2,c(2)),(3,c(3)),...,(n,c(n))\} - (1,n) \\ &= \{(1,c(2)),(2,c(3)),...,(n-1,c(n))\} \end{aligned}$$

  con lo que el vector permutación $[c(2), c(3), ..., c(n)]$ determina el nuevo arreglo Costas.

- Si $(n,n) \in C$ entonces $c(n) = 1$, así

$$\begin{aligned} C_{n-1} &= \{(1,c(1)),(2,c(2)),...,(n-1,c(n-1))\} - (n,n) \\ &= \{(1,c(1)),(2,c(2)),...,(n-1,c(n-1))\} \end{aligned}$$

  con lo que el vector permutación $[c(1), c(2), ..., c(n-1)]$ determina el nuevo arreglo Costas.

En consecuencia al eliminar la correspondiente fila y columna con $c_{ij} = 1$ en cualquiera de las cuatro esquinas, la matriz permutación $(n-1) \times (n-1)$ resultante no pierde las propiedades de arreglo Costas de la matriz permutación de tamaño $n \times n$. □

Ejemplo 1.3.1. *Dados los siguientes arreglos Costas*

- $C_5 = \{(1,1),(2,5),(3,4),(4,2),(5,3)\}$ *en* $[1,5] \times [1,5]$. *Observe que* $(1,1) \in C$. *Al eliminar la fila 1 y columna 1 el conjunto* $C_4 = \{(1,4),(2,3),(3,1),(4,2)\}$ *es un arreglo Costas, como se ilustra en la Figura* 1.6

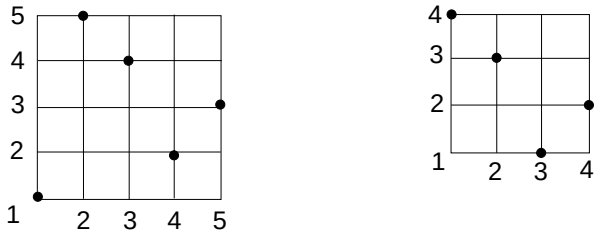


Figura 1.6: Representación de arreglos Costas $C_5 = \{(1,1),(2,5),(3,4),(4,2),(5,3)\}$ (izquierda) y $C_4 = \{(1,4),(2,3),(3,1),(4,2)\}$ (derecha).

- $C_5 = \{(1,2),(2,3),(3,5),(4,4),(5,1)\}$ *en* $[1,5] \times [1,5]$. *Observe que* $(n,1) \in C$. *Al eliminar la fila 5 y columna 1, el conjunto* $C_4 = \{(1,1),(2,2),(3,4),(4,3)\}$ *es un arreglo Costas, como se ilustra en la Figura* 1.7

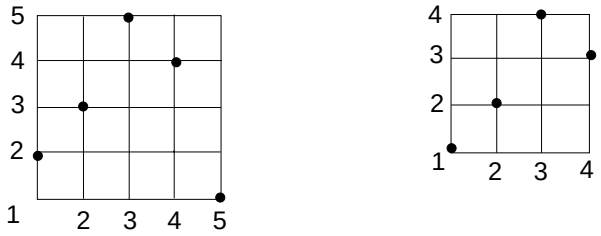


Figura 1.7: Representación de arreglos Costas $C_5 = \{(1,2),(2,3),(3,5),(4,4),(5,1)\}$ (izquierda) y $C_4 = \{(1,1),(2,2),(3,4),(4,3)\}$ (derecha).

- $C_5 = \{(1,5),(2,1),(3,3),(4,4),(5,2)\}$ *en* $[1,5] \times [1,5]$. *Observe que* $(1,n) \in C$. *Al eliminar la fila 1 y columna 5, el conjunto* $C_4 = \{(1,1),(2,3),(3,4),(4,2)\}$ *es un arreglo Costas, como se ilustra en la Figura* 1.8

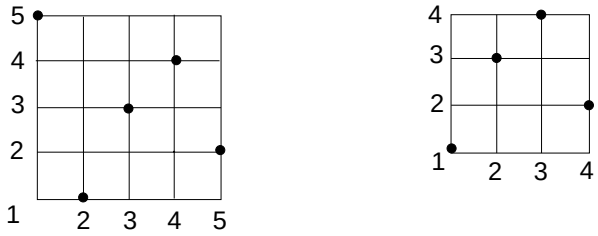


Figura 1.8: Representación de arreglos Costas $C_5 = \{(1,5),(2,1),(3,3),(4,4),(5,2)\}$ (izquierda) y $C_4 = \{(1,1),(2,3),(3,4),(4,2)\}$ (derecha).

- $C_5 = \{(1,4),(2,1),(3,3),(4,2),(5,5)\}$ *en* $[1,5] \times [1,5]$ *. Observe que* $(n,n) \in C$*. Al eliminar la fila 5 y columna 5, el conjunto* $C_4 = \{(1,4),(2,1),(3,3),(4,2)\}$ *es un arreglo Costas, como se ilustra en la Figura* 1.9

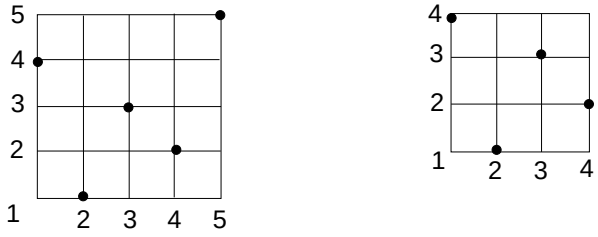


Figura 1.9: Representación de arreglos Costas $C_5 = \{(1,4),(2,1),(3,3),(4,2),(5,5)\}$ (izquierda) y $C_4 = \{(1,4),(2,1),(3,3),(4,2)\}$ (derecha).

Corolario 1.3.1. *De un arreglo Costas de orden* $p-1$ *tipo Welch se obtiene un arreglo Costas de orden* $p-2$ *eliminando la columna y fila correspondiente a* $w_{ij} = 1$*.*

Demostración. Como $g^{p-1} \equiv 1 \pmod{p}$, se tiene que el punto $(p-1,1)$ siempre esta en la esquina inferior derecha del retículo. Por el Lema 1.3.1. se obtiene un arreglo Costas de orden $p-2$. □

Ejemplo 1.3.2. *Con* $p = 7$*,* $g = 3$ *se tiene* $W = \{(1,3),(2,2),(3,6),(4,4),(5,5),(6,1)\}$ *(Welch). Eliminando la columna y fila correspondiente a la esquina* $(6,1)$ *del retículo se obtiene* $C = \{(1,2),(2,1),(3,5),(4,3),(5,4)\}$*, como se ilustra en la Figura* 1.10

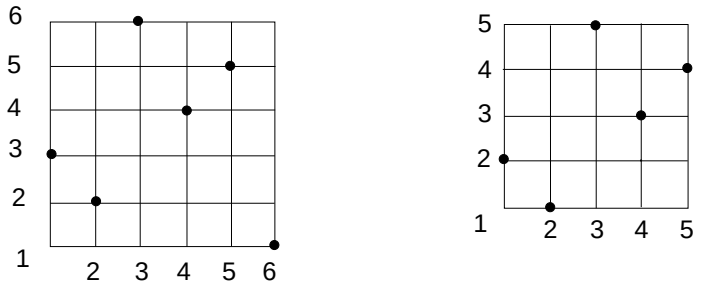


Figura 1.10: Representación de arreglos Costas tipo Welch de orden 6 (izquierda) y arreglo Costas de orden 5 (derecha).

Corolario 1.3.2. *Si* 2 *es una raíz primitiva módulo* p *entonces de la construcción de Welch se puede obtener un arreglo Costas de orden* $p-3$.

Demostración. Como 2 es raíz primitiva se cumple que $2^{p-1} \equiv 1 \pmod{p}$, pero

$$\begin{aligned} 2^{p-1} &= 2(2^{p-2}) \\ &= (2^{p-2}) + (2^{p-2}) \end{aligned}$$

como $2^{p-1} \equiv 1 \pmod{p}$ se tiene que $(p-2, p-2) \in W$.
Así por el Lema 1.3.1 este punto puede ser eliminado obteniendo un arreglo Costas de orden $p-3$. □

Ejemplo 1.3.3. *Con* $p = 11$, $g = 2$ *una raíz primitiva módulo* 11.
$W = \{(1,2),(2,4),(3,8),(4,5),(5,10),(6,9),(7,7),(8,3),(9,6),(10,1)\}$ *es un arreglo Costas de orden* 10*, de éste eliminando el punto* $(10,1)$ *se obtiene un arreglo Costas de orden 9 dado por* $C = \{(1,1),(2,3),(3,7),(4,4),(5,9),(6,8),(7,6),(8,2),(9,5)\}$ *y eliminando* $(1,1)$ *se tiene* $C = \{(1,2),(2,6),(3,3),(4,8),(5,7),(6,5),(7,1),(8,4)\}$ *arreglo Costas de orden 8, como se ilustra en la Figura* 1.11

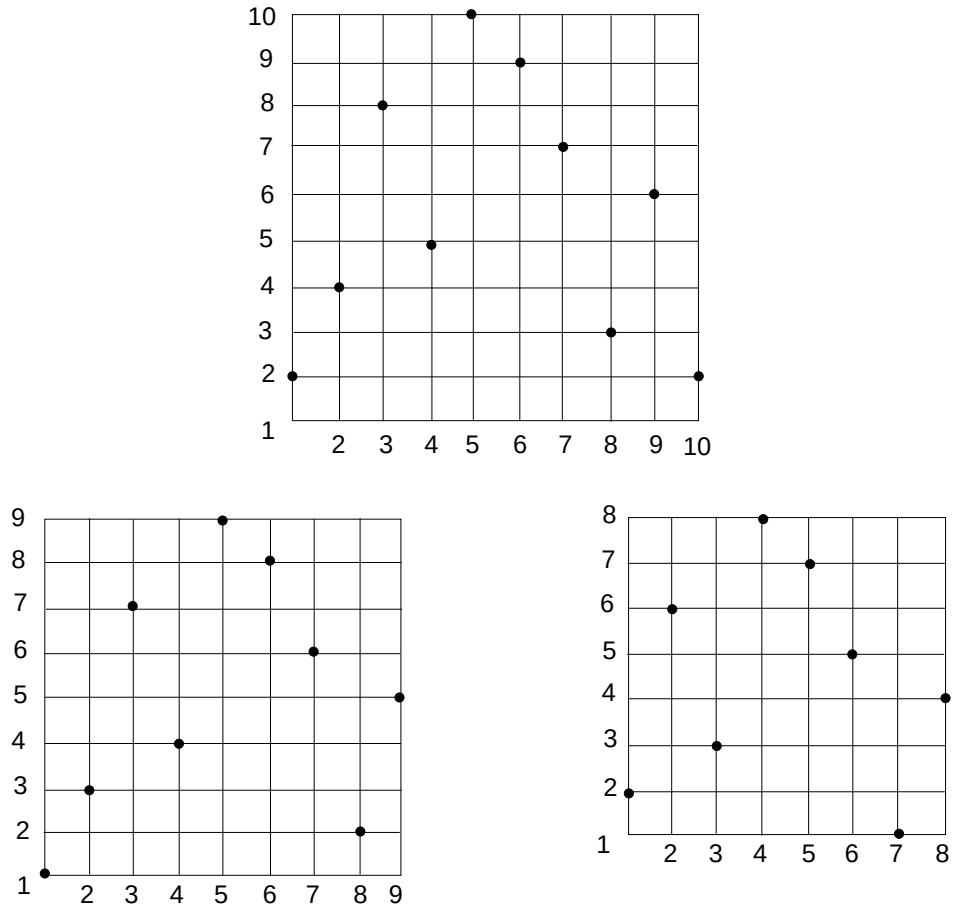


Figura 1.11: Representación de arreglos Costas tipo Welch de orden 10 (arriba), arreglo Costas de orden 9 (izquierda) y arreglo Costas de orden 8 (derecha).

Corolario 1.3.3. *Cada permutación cíclica de las filas de un arreglo Costas tipo Welch es de nuevo un arreglo Costas de orden* $p-1$.

Demostración. Sean g una raíz primitiva modulo p, b cualquier entero positivo fijo. Entonces la matriz permutación $(p-1)\times(p-1)$ con $w_{ij}=1$ si y solo si $j \equiv g^{i+b} \pmod{p}$ es un arreglo Costas. Se debe probar que la matriz permutación es un arreglo Costas de orden $p-1$.

Suponga que no es un arreglo Costas entonces se puede encontrar dos pares de puntos de la siguiente forma

$$\left\{(i, \alpha^{i+b}), (i+k, \alpha^{i+c+k})\right\}$$

$$\left\{(l, \alpha^{l+b}), (l+k, \alpha^{l+c+k})\right\}$$

con $i \neq l$, de donde

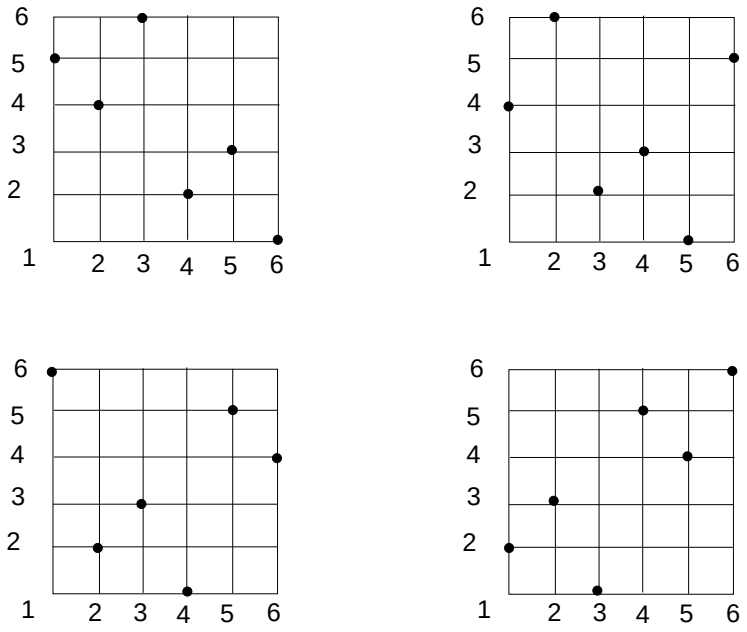
$$(k, \alpha^{i+b+k} - \alpha^{i+b}) = (k, \alpha^{l+b+k} - \alpha^{l+b})$$

con $1 \leq k \leq p-2$, así $\alpha^{i+b}(\alpha^k - 1) = \alpha^{l+b}(\alpha^k - 1)$, pero $\alpha^k - 1 \not\equiv 0 \pmod{p}$, luego $\alpha^{i+b} = \alpha^{l+b}$, en consecuencia $i = l$.

Por tanto la matriz permutación es un arreglo Costas de orden $p-1$. □

Ejemplo 1.3.4. *En el arreglo Costas de orden 6,* $W = \{(1,5),(2,4),(3,6),(4,2),(5,3),(6,1)\}$ *donde la permutación asociada es* $[5,4,6,2,3,1]$ *con* $p = 7$ *y* $g = 5$*, al permutar las filas se obtienen de nuevo arreglos Costas del mismo orden, como se ilustra en la Figura* 1.12

$$\begin{aligned}[5,4,6,2,3,1] &\rightarrow [4,6,2,3,1,5] \rightarrow [6,2,3,1,5,4] \rightarrow [2,3,1,5,4,6] \\ &\rightarrow [3,1,5,4,6,2] \rightarrow [1,5,4,6,2,3]\,.\end{aligned}$$



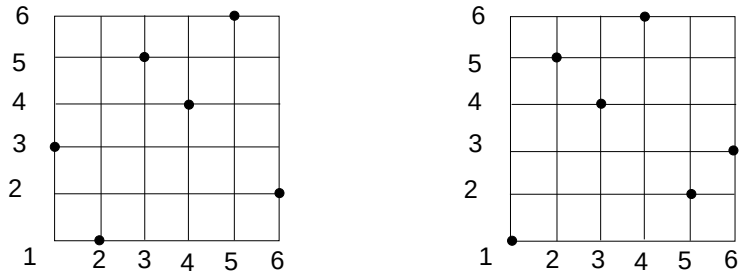


Figura 1.12: Permutación de filas de un arreglos Costas tipo Welch de orden 6, $W = [5, 4, 6, 2, 3, 1]$ (arriba izquierda), $C = [4, 6, 2, 3, 1, 5]$ (arriba derecha), $C = [6, 2, 3, 1, 5, 4]$ (medio derecha), $C = [2, 3, 1, 5, 4, 6]$ (medio izquierda), $C = [3, 1, 5, 4, 6, 2]$ (abajo derecha), $C = [1, 5, 4, 6, 2, 3]$ (abajo izquierda).

Nota 1.3.1. Las propiedades de un arreglo Costas se conservan bajo la acción del grupo de simetrías del cuadrado ($\mathbb{D}_4$).

Corolario 1.3.4. *Si* 2 *es una raíz primitiva módulo* p *entonces de la construcción de Lempel se puede obtener un arreglo Costas de orden* $p - 3$.

Demostración. (Análoga al Corolario 1.3.2.) □

Ejemplo 1.3.5. *Dado el arreglo Costas de orden 9*
$L = \{(1, 5), (2, 3), (3, 2), (4, 7), (5, 1), (6, 8), (7, 4), (8, 6), (9, 9)\}$ (*ver Ejemplo* 1.3.1 *con* $q = 11$ *y* $\alpha = 2$)*, eliminando la fila y columna correspondiente al punto* $(9, 9)$ *se obtiene un arreglo Costas* $C = \{(1, 5), (2, 3), (3, 2), (4, 7), (5, 1), (6, 8), (7, 4), (8, 6)\}$ *de orden* 8*, como se iliustra en la Figura* 1.13

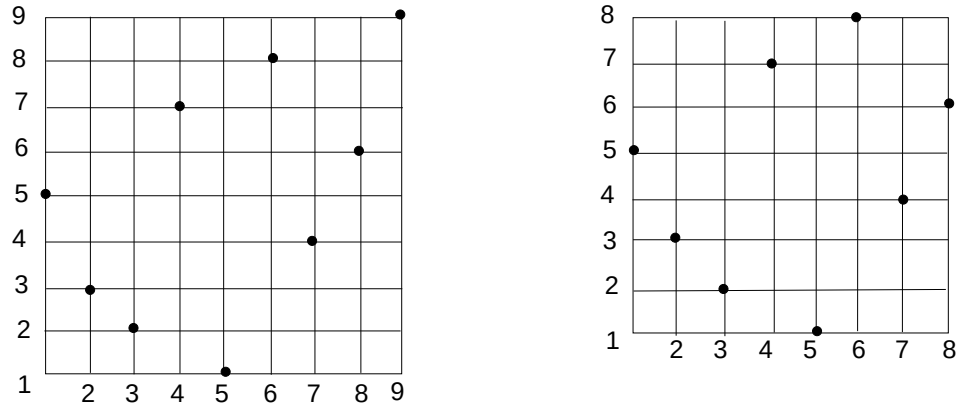


Figura 1.13: Representación de arreglos Costas tipo Lempel de orden 9 (izquierda) y arreglo Costas de orden 8 (derecha).

Teorema 1.3.1. *Si en un arreglo Costas tipo Golomb de orden $q-2$ se cumple que $\alpha+\beta=1$ (α y β no necesariamente distintas), entonces de este se puede obtener un arreglo Costas de orden $q-3$.*

Demostración.

$$\begin{aligned} \alpha+\beta=1 &\Leftrightarrow \beta=1-\alpha \\ &\Leftrightarrow (1,\log_\beta(1-\alpha))\in G_{(\alpha,\beta)} \\ &= (1,\log_\beta(\beta))\in G_{(\alpha,\beta)} \\ &= (1,1)\in G_{(\alpha,\beta)}. \end{aligned}$$

Así por el Lema 1.3.1 este punto puede ser eliminado obteniendo un arreglo Costas de orden $q-3$. □

Ejemplo 1.3.6. *Para $q=7$ con $\alpha=3$ y $\beta=5$ se tiene $\alpha+\beta=1$, luego $G=\{(1,1),(2,3),(3,4),(4,2),(5,5)\}$ es un arreglo Costas de orden 5. Por el Lema 1.3.1 la correspondiente fila y columna al punto $(1,1)$ puede ser eliminado y obtener un arreglo Costas $C=\{(1,2),(2,3),(3,1),(4,4)\}$ de orden 4, como se ilustra en la Figura 1.14*

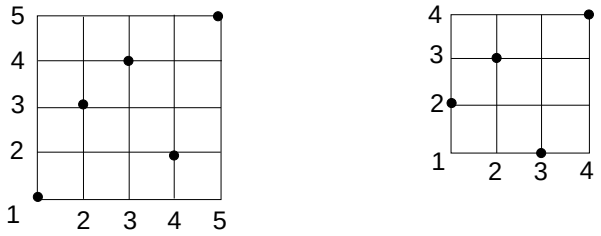


Figura 1.14: Representación de arreglos Costas tipo Golomb de orden 5 (izquierda) y arreglo Costas de orden 4 (derecha).

Teorema 1.3.2. *Si el campo $\mathbb{F}_{2^k}$ tiene dos raíces primitivas α y β, $\alpha+\beta=1$, el arreglo Costas de orden 2^k-2 tipo Golomb puede ser reducido a un arreglo Costas de orden 2^k-3 y este a su vez en uno de orden 2^k-4.*

Demostración. Sea $q=2^t$, $char(\mathbb{F}_q)=2$ (Característica 2), entonces $(\alpha+\beta)^2=\alpha^2+\beta^2$, como $\alpha+\beta=1 \Rightarrow \alpha^2+\beta^2=1$. Ahora si

- $\alpha+\beta=1$ entonces $(1,1)\in G$.
- $\alpha^2+\beta^2=1$ entonces $(2,\log_\beta(1-\alpha^2))=(2,\log_\beta(\beta^2))=(2,2)\in G$.

Así por el Lema 1.3.1. los puntos (1,1) y (2,2) pueden ser eliminados obteniendo un arreglo Costas de orden 2^k-3 y 2^k-4 respectivamente. □

Capítulo 2

Arreglos Costas Como Conjuntos De Sidon Especiales

En este capítulo se presenta la definición y las construcciones de arreglos Costas desde los conjuntos de Sidon. Y se hace un análisis detallado a la construcción de Welch.
Sea $< G, + >$ grupo conmutativo (Grupo ambiente), notado aditívamente, y $S \subseteq G$.

2.1. Conceptos, Notación Y Ejemplos

Definición 2.1.1. *El* **conjunto suma** *de S, notado $S + S$ se define como el conjunto de todas las sumas de dos elementos en S, es decir: $S + S := \{a + b : a, b \in S\}$.*

Dado $S = \{s_1, s_2, ..., s_n\}$, la entrada ij-ésima del conjunto suma está dada por $s_i + s_j$. La Tabla 2.1 ilustra la representación para $n = 3$.

$+$	s_1	s_2	s_3
s_1	$s_1 + s_1$	$s_1 + s_2$	$s_1 + s_3$
s_2	$s_2 + s_1$	$s_2 + s_2$	$s_2 + s_3$
s_3	$s_3 + s_1$	$s_3 + s_2$	$s_3 + s_3$

Tabla 2.1: Suma $S + S$

Ejemplo 2.1.1. *Sea* $S = \{0, 1, 3, 5, 7\} \subseteq \mathbb{Z}$. *La Tabla* 2.2 *muestra el conjunto* $S + S$ *de sumas es:*

+	0	1	3	5	7
0	0	1	3	5	7
1	1	2	4	6	8
3	3	4	6	8	10
5	5	6	8	10	12
7	7	8	10	12	14

Tabla 2.2: Sumas.

donde el conjunto suma $S + S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14\}$.

Definición 2.1.2. *El* **conjunto diferencia** *de* S, *notado* $S-S$ *se define como el conjunto de todas las diferencias de dos elementos en* S, *es decir:* $S - S := \{a - b : a, b \in S\}$.

Dado $S = \{s_1, s_2, ..., s_n\}$, la entrada ij-ésima del conjunto diferencia está dada por: $s_i - s_j$. La Tabla 2.3 representa las diferencias para $n = 3$

-	s_1	s_2	s_3
s_1	$s_1 - s_1$	$s_1 - s_2$	$s_1 - s_3$
s_2	$s_2 - s_1$	$s_2 - s_2$	$s_2 - s_3$
s_3	$s_3 - s_1$	$s_3 - s_2$	$s_3 - s_3$

Tabla 2.3: Diferencias $S - S$

Ejemplo 2.1.2. *Sea* $S = \{0, 1, 3, 5, 7\} \subseteq \mathbb{Z}$. *La Tabla* 2.4 *representa las diferencias de* S

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

Tabla 2.4: Diferencias.

Y el conjunto de diferencias es $S - S = \{-7, -6, -5, -4, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7\}$.

Definición 2.1.3. *S es un* **conjunto con diferencias distintas** *en G si todas las diferencias de dos elementos diferentes de S son distintos. Es decir si para todo $a, b, a', b' \in S$ con $a \neq b$ y $a' \neq b'$ se tiene que*

$$a - b = a' - b' \Rightarrow \{a, b\} = \{a', b'\}.$$

Ejemplo 2.1.3. *Sea $S = \{0, 1, 3, 6, 10\} \subseteq \mathbb{Z}$.La Tabla 2.5 representa las diferencias de S*

-	0	1	3	6	10
0	0	-1	-3	-6	-10
1	1	0	-2	-5	-9
3	3	2	0	-3	-7
6	6	5	3	0	-4
10	10	9	7	4	0

Tabla 2.5: Diferencias distintas de $S = \{0, 1, 3, 6, 10\}$.

de donde se verifica que S es un conjunto de diferencias distintas.

Definición 2.1.4. *S es un* **conjunto de Sidon** *en G (conjunto B_2 en G) si todas las sumas de dos elementos de S son distintas. Es decir si para todo $a, b, a', b' \in S$ se tiene que*

$$a + b = a' + b' \Rightarrow \{a, b\} = \{a', b'\}.$$

Ejemplo 2.1.4. *El conjunto $S = \{0, 2, 3, 7, 20, 26\}$ es un conjunto de Sidon en $\mathbb{Z}$ ya que todas las sumas de dos elementos de S son distintas como se ilustra en la Tabla 2.6*

+	0	2	3	7	20	26
	0	2	3	7	20	26
		4	5	9	22	28
			6	10	23	29
				14	27	33
					40	46
						52

Tabla 2.6: Sumas distintas de $S = \{0, 2, 3, 7, 20, 26\}$.

Comentarios 2.1.1 Si S es un conjunto finito, con k elementos, se denota $|S| = k$. Con esta notación se puede ver

1. S es un conjunto de Sidon si y sólo si

$$|S + S| = \binom{k}{2} + k = \binom{k+1}{2} = \frac{k(k+1)}{2}.$$

2. Si en G no hay elementos de orden dos, distintos de cero, S es un conjunto con diferencias distintas si y sólo si

$$|S - S| = 2\binom{k}{2} + 1 = k(k-1) + 1.$$

Teorema 2.1.1. *Suponga que G no tiene elementos de orden dos*[1]*. S es un conjunto de Sidon en G si y sólo si S es un conjunto de diferencias distintas en G.*

Demostración. ($\Rightarrow$) Sean $a, b, a', b' \in S$ con $a \neq b$ y $a' \neq b'$, tales que si $a - b = a' - b'$ entonces $a + b' = a' + b$.

Como S es un conjunto de Sidon en G se tiene que $\{a, b'\} = \{a', b\}$.

Ahora, como $a \neq b$ se debe tener $a = a'$ y $b = b'$, luego $\{a, b\} = \{a', b'\}$.

Es decir es un conjunto de diferencias distintas.

($\Leftarrow$) Sean $a, b, a', b' \in S$ tal que si $a + b = a' + b'$ entonces $a - a' = b - b'$.

[1] G no tiene elementos de orden dos, significa que $(a + a = 0 \Leftrightarrow a = 0)$.

(i) Si $a \neq a'$, $b \neq b'$ y como S es de diferencias distintas $\{a, a'\} = \{b, b'\}$.

Luego ($a = b$ y $a' = b'$) o ($a = b'$ y $a' = b$).

Si $a = b$ y $a' = b'$ entonces $a + a = a' + a' \neq 0$, luego $a = a'$ lo cual no es posible.

Por tanto $a = b'$ y $a' = b$ y así $\{a, b\} = \{a', b'\}$.

(ii) Si $a = a'$, $b = b'$. Es claro que $\{a, b\} = \{a', b'\}$. □

Lema 2.1.1. *Sean $(A, +, \cdot)$ un anillo con identidad y sea A^* su grupo de unidades. Si $S \subseteq A$ es un conjunto de Sidon en $(A, +)$, $u \in A^*$ y $t \in A$ entonces*

$$uS + t := \{ux + t : x \in S\}$$

es un conjunto de Sidon en $(A, +)$.

Demostración. Suponga que $x_1, x_2, x_3, x_4 \in S$ son tales que

$$(ux_1 + t) + (ux_2 + t) = (ux_3 + t) + (ux_4 + t),$$

entonces $u(x_1 + x_2) = u(x_3 + x_4)$. Como $u \in A^*$, también $x_1 + x_2 = x_3 + x_4$ y ya que S es un conjunto de Sidon se sigue que $\{x_1, x_2\} = \{x_3, x_4\}$, de donde $\{ux_1 + t, ux_2 + t\} = \{ux_3 + t, ux_4 + t\}$. □

Definición 2.1.5. *Un conjunto $C \subseteq [1, n]^2$ es un arreglo Costas de orden n si satisface las siguientes condiciones:*

(1) $|C| = n$

(2) *Para cada $i \in [1, n]$ existe un único $j \in [1, n]$ tal que $(i, j) \in C$*

(3) *C es un conjunto de Sidon en el grupo $(\mathbb{Z}^2, +)$.*

Comentario 2.1.2 Las condiciones (1) y (2) permiten identificar al conjunto C como una **Permutación** de $[1, n]$. (Biyección de $[1, n]$ en $[1, n]$).

Ejemplo 2.1.5. *El conjunto $C = \{(1, 5), (2, 2), (3, 6), (4, 1), (5, 3), (6, 4)\}$ es un arreglo Costas de orden seis.*

La permutación asociada es

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 3 & 4 \end{pmatrix}$$

mientras que el conjunto de diferencias se representa en la Tabla 2.7

−	(1, 5)	(2, 2)	(3, 6)	(4, 1)	(5, 3)	(6, 4)
(1, 5)	(0, 0)	(1,-3)	(2, 1)	(3,-4)	(4,-2)	(5,-1)
(2, 2)	(-1,3)	(0, 0)	(1, 4)	(2,-1)	(3, 1)	(4, 2)
(3, 6)	(-2,-1)	(-1,-4)	(0, 0)	(1,-5)	(2,-3)	(3,-2)
(4, 1)	(-3,4)	(-2,1)	(-1,5)	(0, 0)	(1, 2)	(2, 3)
(5, 3)	(-4,2)	(-3,-1)	(-2,3)	(-1,-2)	(0, 0)	(1, 1)
(6, 4)	(-5,1)	(-4,-2)	(-3,2)	(-2,-3)	(-1,-1)	(0, 0)

Tabla 2.7: Diferencias distintas de $C = \{(1,5),(2,2),(3,6),(4,1),(5,3),(6,4)\}$

Lema 2.1.2. *Sea $(\mathbb{F},+,\cdot)$ un campo y sean $x,y,u,v \in \mathbb{F}$. Entonces $xy = uv$ y $x+y = u+v$ si y sólo si $x = u, y = v$ o $x = v, y = u$.*

Demostración. ($\Leftarrow$) Inmediata.
($\Rightarrow$) Si $P = xy = uv$, $T = x + y = u + v$, entonces x, y y u, v son raíces del polinomio $Z^2 - TZ + P = (Z-x)(Z-y) = (Z-u)(Z-v)$, de donde $x = u, y = v$ o $x = v, y = u$. □

2.2. Construcción General De Welch

Sean p un primo, y α una raíz primitiva módulo p.

Teorema 2.2.1. *Los conjuntos:*

1. $W_1(p,\alpha) := \{(i, \alpha^i) : i = 1, 2, ..., p-1\}$
2. $W_1^T(\alpha,p) := \{(\alpha^i, i) : i = 1, 2, ..., p-1\}$

son conjuntos de Sidon con $p-1$ elementos en $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +)$ y $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$, respectivamente.

Demostración. Sean p, α fijos.

1. Primero se probará que $|W_1(p,\alpha)| = p-1$.
   Si $(i, \alpha^i) = (j, \alpha^j)$; con $1 \leq i, j \leq p-1$, entonces

$$i \equiv j \pmod{p-1}$$
$$i - j \equiv j - i \equiv 0 \pmod{p-1}$$
$$(p-1) \text{ divide a } |i-j|$$

entonces $i - j = 0$ de donde $i = j$.

Se debe probar que $W_1(p, \alpha)$ es un conjunto de Sidon en $\mathbb{Z}_{p-1} \times Z_p$. Sea $(i, \alpha^i) + (j, \alpha^j) = (k, \alpha^k) + (l, \alpha^l)$ en $\mathbb{Z}_{p-1} \times Z_p$, luego $(i+j, \alpha^i + \alpha^j) = (k+l, \alpha^k + \alpha^l)$ de donde

$$i + j \equiv k + l \pmod{p-1},$$

así que en $\mathbb{Z}_p$,

$$\alpha^{i+j} = \alpha^{k+l}$$

es decir

$$\alpha^i \alpha^j = \alpha^k \alpha^l. \tag{2.1}$$

Por otro lado en $\mathbb{Z}_p$

$$\alpha^i + \alpha^j = \alpha^k + \alpha^l. \tag{2.2}$$

De (2.1) y (2.2), por el Lema 2.1.2, $\{\alpha^i, \alpha^j\} = \{\alpha^k, \alpha^l\}$ y también $\{i, j\} = \{k, l\}$. Por tanto $\{(i, \alpha^i), (j, \alpha^j)\} = \{(k, \alpha^k), (l, \alpha^l)\}$, así $W_1(p, \alpha)$ es un conjunto de Sidon en $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$.

2. La demostración es análoga. □

Como el grupo de unidades $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)$ es

$$\begin{aligned}(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^* &= \mathbb{Z}_{p-1}^* \times \mathbb{Z}_p^* \\ &= \{(u, v) : 1 \leq u < p-1, 1 \leq v \leq p-1, mcd(u, p-1) = 1\},\end{aligned}$$

por el Lema 2.1.2 se tiene el siguiente resultado.

Corolario 2.2.1. *Para todo $(u, v) \in (\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*$, los conjuntos*

1. $W_1(p, \alpha, u, v) = \{(ui, v\alpha^i) : 1 \leq i \leq p-1\} = (u, v)W_1(p, \alpha)$,

2. $W_1^T(p,\alpha,v,u) = \{(v\alpha^i, ui) : 1 \leq i \leq p-1\} = (v,u)W_1^T(p,\alpha)$.

son conjuntos de Sidon con $p-1$ *elementos en* $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +)$ *y en* $(\mathbb{Z}_p \times \mathbb{Z}_{p-1}, +)$ *respectivamente.*

Nota 2.2.1. Como $W_1(p,\alpha) \subseteq \mathbb{Z}_{p-1} \times \mathbb{Z}_p^*$, y $|W_1(p,\alpha)| = p-1$, y también $< \alpha >_p = \mathbb{Z}_p^*$, es claro que $W_1(p,\alpha)$ corresponde a la construcción de Welch (Sección 1.2). Esto también es válido para $W_1^T(p,\alpha)$ y para cada uno de los conjuntos del Corolario 2.2.1.

Ejemplo 2.2.1. *Sea* $p = 7$ *y* $\alpha = 3$, $u \in$ [1,6], $mcd(u,6) = 1$, $u = \{1,5\}$, $v \in [1,6]$. *Entonces se tienen los siguientes arreglos Costas de orden* 6, *tipo Welch, como se muestra en la Tabla* 2.8

u	v	$W(7,3,u,v)$	Permutación	Transpuesto
	1	$(i, 1\cdot 3^i)$: (1,3), (2,2), (3,6), (4,4), (5,5), (6,1)	[3,2,6,4,5,1]	[6,2,1,4,5,3]
	2	$(i, 2\cdot 3^i)$: (1,6), (2,4), (3,5), (4,1), (5,3), (6,2)	[6,4,5,1,3,2]	[4,6,5,2,3,1]
	3	$(i, 3\cdot 3^i)$: (1,2), (2,6), (3,4), (4,5), (5,1), (6,3)	[2,6,4,5,1,3]	[5,1,6,3,4,2]
1	4	$(i, 4\cdot 3^i)$: (1,5), (2,1), (3,3), (4,2), (5,6), (6,4)	[5,1,3,2,6,4]	[2,4,3,6,1,5]
	5	$(i, 5\cdot 3^i)$: (1,1), (2,3), (3,2), (4,6), (5,4), (6,5)	[1,3,2,6,4,5]	[1,3,2,5,6,4]
	6	$(i, 6\cdot 3^i)$: (1,4), (2,5), (3,1), (4,3), (5,2), (6,6)	[4,5,1,3,2,6]	[3,5,4,1,2,6]
	1	$(5i, 1\cdot 3^i)$: (5,3), (4,2), (3,6), (2,4), (1,5), (6,1)	[5,4,6,2,3,1]	[6,4,5,2,1,3]
	2	$(5i, 2\cdot 3^i)$: (5,6), (4,4), (3,5), (2,1), (1,3), (6,2)	[3,1,5,4,6,2]	[2,6,1,4,3,5]
	3	$(5i, 3\cdot 3^i)$: (5,2), (4,6), (3,4), (2,5), (1,1), (6,3)	[1,5,4,6,2,3]	[1,5,6,3,2,4]
5	4	$(5i, 4\cdot 3^i)$: (5,5), (4,1), (3,3), (2,2), (1,6), (6,4)	[6,2,3,1,5,4]	[4,2,3,6,5,1]
	5	$(5i, 5\cdot 3^i)$: (5,1), (4,3), (3,2), (2,6), (1,4), (6,5)	[4,6,2,3,1,5]	[5,3,4,1,6,2]
	6	$(5i, 6\cdot 3^i)$: (5,4), (4,5), (3,1), (2,3), (1,2), (6,6)	[2,3,1,5,4,6]	[3,1,2,5,4,6]

Tabla 2.8: Construcción de arreglos Costas de orden 6, tipo Welch, con $p = 7$ y $\alpha = 3$.

Observaciones Sea $W_1(\alpha)$ en lugar de $W_1(p,\alpha)$ y $W_1(\beta)$ en lugar de $W_1(p,\beta)$

I) *Sean* α, β *raíces primitivas módulo* p $(\alpha \neq \beta)$, *los conjuntos*

$$W_1(\alpha) := \left\{(i, \alpha^i) : i = 1, 2, ...p-1\right\},$$

$$W_1(\beta) := \left\{(i, \beta^i) : i = 1, 2, ...p-1\right\}$$

están relacionados de la siguiente forma

$$W_1(\beta) = (u, v)W_1(\alpha),$$

donde $(u, v) = ((\log_\alpha(\beta))^{-1}, 1) \in (\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*$, $(u, v)^{-1} = \{(\log_\alpha(\beta)), 1)\}$, así

$$W_1(\alpha) = (\log_\alpha(\beta), 1)W_1(\beta),$$

$$W_1(\beta) = (\log_\beta(\alpha), 1)W_1(\alpha).$$

Es decir todo elemento de $W_1(\alpha)$ es elemento de $W_1(\beta)$ y viceversa.
Sea $(j, \beta^j) \in W_1(\beta)$, con $i = (\log_\beta(\alpha))^{-1}j$, es decir $j = (\log_\beta(\alpha))i$ con lo que

$$\begin{aligned}
(j, \beta^j) &= \left((\log_\beta(\alpha))i, \beta^{(\log_\beta(\alpha))i}\right) \\
&= \left((\log_\beta(\alpha))i, \left(\beta^{\log_\beta(\alpha)}\right)^i\right) \\
&= \left((\log_\beta(\alpha))i, \alpha^i\right) \\
&= \left((\log_\beta(\alpha)), 1\right)\left(i, \alpha^i\right) \quad \in \left((\log_\beta(\alpha)), 1\right) W_1(\alpha).
\end{aligned}$$

De la misma manera los conjuntos

$$W_1^T(\alpha) := \left\{(i, \alpha^i) : i = 1, 2, ...p - 1\right\},$$

$$W_1^T(\beta) := \left\{(i, \beta^i) : i = 1, 2, ...p - 1\right\},$$

están relacionados mediante

$$W_1^T(\beta) = (v, u)W_1^T(\alpha),$$

donde (u, v) se definió anteriormente.

Comentario 2.2.1. El cambio de la raíz primitiva es equivalente a multiplicar por una unidad adecuada.

Ejemplo 2.2.2. *Sea* $p = 7$ *y* $\beta = 5$, $u \in$ [1,6], $mcd(u, 6) = 1$, $u \in \{1, 5\}$, $v \in [1, 6]$. *Entonces se tienen los siguientes arreglos Costas de orden* 6 *tipo Welch, como se muestra en la Tabla* 2.9

Se observa que los vectores permutación obtenidos en este ejemplo pueden obtenerse de los vectores permutación del Ejemplo 2.2.1. multiplicando cada conjunto por la unidad adecuada. Análogamente para los vectores transpuestos.

u	v	$W(7,5,u,v)$	permutación	Transpuesto
	1	$(i, 1\cdot 5^i)$: (1,5), (2,4), (3,6), (4,2), (5,3), (6,1)	[5,4,6,2,3,1]	[6,4,5,2,1,3]
	2	$(i, 2\cdot 5^i)$: (1,3), (2,1), (3,5), (4,4), (5,6), (6,2)	[3,1,5,4,6,2]	[2,6,1,4,3,5]
	3	$(i, 3\cdot 5^i)$: (1,1), (2,5), (3,4), (4,6), (5,2), (6,3)	[1,5,4,6,2,3]	[1,5,6,3,2,4]
1	4	$(i, 4\cdot 5^i)$: (1,6), (2,2), (3,3), (4,1), (5,5), (6,4)	[6,2,3,1,5,4]	[4,2,3,6,5,1]
	5	$(i, 5\cdot 5^i)$: (1,4), (2,6), (3,2), (4,3), (5,1), (6,5)	[4,6,2,3,1,5]	[5,3,4,1,6,2]
	6	$(i, 6\cdot 5^i)$: (1,2), (2,3), (3,1), (4,5), (5,4), (6,6)	[2,3,1,5,4,6]	[3,1,2,5,4,6]
	1	$(5i, 1\cdot 5^i)$: (5,5), (4,4), (3,6), (2,2), (1,3), (6,1)	[3,2,6,4,5,1]	[6,2,1,4,5,3]
	2	$(5i, 2\cdot 5^i)$: (5,3), (4,1), (3,5), (2,4), (1,6), (6,2)	[6,4,5,1,3,2]	[4,6,5,2,3,1]
	3	$(5i, 3\cdot 5^i)$: (5,1), (4,5), (3,4), (2,6), (1,2), (6,3)	[2,6,4,5,1,3]	[5,1,6,3,4,2]
5	4	$(5i, 4\cdot 5^i)$: (5,6), (4,2), (3,3), (2,1), (1,5), (6,4)	[5,1,3,2,6,4]	[2,4,3,6,1,5]
	5	$(5i, 5\cdot 5^i)$: (5,4), (4,6), (3,2), (2,3), (1,1), (6,5)	[1,3,2,6,4,5]	[1,3,2,5,6,4]
	6	$(5i, 6\cdot 5^i)$: (5,2), (4,3), (3,1), (2,5), (1,4), (6,6)	[4,5,1,3,2,6]	[3,5,4,1,2,6]

Tabla 2.9: Construcción de arreglos Costas de orden 6, tipo Welch, con $p = 7$ y $\beta = 5$.

II) *En* $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +, \cdot)$ *anillo conmutativo con unidad.*

Si $\varphi(p-1) \geq 2$, *entonces* $\left|(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)\right|^* = \varphi(p-1)(p-1) \geq 2(p-1) \geq 4$.

Así por lo menos hay 4 unidades $(\pm 1, \pm 1)$, lo que significa que hay al menos 4 arreglos Costas.

$$\left.\begin{aligned} W_1(\alpha) &= (1,1)W_1(\alpha) \\ &= (1,-1)W_1(\alpha) \\ &= (-1,1)W_1(\alpha) \\ &= (-1,-1)W_1(\alpha) \end{aligned}\right\} \text{ rotaciones } 90^o,\ 180^o,\ 270^o,\ 360^o.$$

Al igual que

$$\left.\begin{aligned} W_1^T(\alpha) &= (1,1)W_1^T(\alpha) \\ &= (1,-1)W_1^T(\alpha) \\ &= (-1,1)W_1^T(\alpha) \\ &= (-1,-1)W_1^T(\alpha) \end{aligned}\right\} \text{ rotaciones } 90^o,\ 180^o,\ 270^o,\ 360^o.$$

III) *De unidades distintas se obtienen conjuntos distintos. Es decir*

$$(u_1, v_1)W_1(\alpha) = (u_2, v_2)W_1(\alpha) \Leftrightarrow (u_1, v_1) = (u_2, v_2).$$

Demostración. ($\Leftarrow$) Inmediato.
($\Rightarrow$) Suponga que $(u_1, v_1)W_1(\alpha) = (u_2, v_2)W_1(\alpha)$

- $i = p-1$, como $u_1(p-1) = p-1$ ($p-1$ es el cero en $\mathbb{Z}_{p-1}$) y $\alpha^{p-1} = 1$, esto es $v_1(\alpha^{p-1}) = v_1$. Luego
  $(p-1, v_1) = (u_1, v_1)(p-1, \alpha^{p-1}) \in (u_1, v_1)W_1(\alpha) = (u_2, v_2)W_1(\alpha)$, luego
  $(p-1, v_1) = (u_2 j, v_2\alpha^j)$ es posible sólo si $j = p-1$ y así $v_2 = v_1$.
- $i = 1$, $(u_1, v_1)(1, \alpha) \in (u_1, v_1)W_1(\alpha) = (u_2, v_2)W_1(\alpha)$, luego $(u_1, v_1\alpha) = (u_2 j, v_2\alpha^j)$ y como $v_2 = v_1$, se tiene que $j = 1$ y así $u_2 = u_1$.

Por tanto $(u_1, v_1) = (u_2, v_2)$. □

Ejemplo 2.2.3. *Se puede observar que en los Ejemplos* 2.2.1 *y* 2.2.2 *con unidades distintas se obtuvo conjuntos distintos.*

IV) *Para todo primo $p > 3$ los conjuntos $W_1(p, \alpha)$ no son simétricos.*

Demostración. Sean $W_1(\alpha)$ y $W_1^T(\alpha)$ tales que $W_1(\alpha) = \{(i, \alpha^i) : i = 1, 2, ..., p-1\}$ y $W_1^T(\alpha) = \{(\alpha^j, j) : j = 1, 2, ..., p-1\}$. Suponga que $W_1(\alpha) = W_1^T(\alpha)$,
como $(1, \alpha) \in W_1(\alpha)$, debemos tener que $(1, \alpha) = (\alpha^j, j)$ para algún $j = 1, 2, ..., p-1$, entonces $\alpha^j = 1$ y $\alpha = j$, esto es $j = p-1 = \alpha$.
Como $p - 1 = -1 \pmod p$, se tiene que $\alpha = -1$ es raíz primitiva módulo p, y como para todo primo p se cumple $(-1)^2 \equiv 1 \pmod p$, entonces $p = 3$.
Esto significa que para todo primo $p > 3$, los conjuntos $W_1(p, \alpha)$ no son simétricos. □

CONCLUSIÓN. Para todo primo p hay $\varphi(p-1)(p-1) = \left|(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*\right|$ arreglos Costas tipo Welch de orden $p-1$. Similarmente hay $(p-1)\varphi(p-1) = \left|(\mathbb{Z}_p \times \mathbb{Z}_{p-1})^*\right|$ arreglos Costas tipo Welch transpuestos de orden $p-1$. En total hay al menos $2\varphi(p-1)(p-1)$ arreglos costas de orden $p-1$. Es decir, si $\mathcal{C}(n)$ cuenta el número total de arreglos Costas de orden n, entonces $\mathcal{C}(p-1) \geq 2(p-1)\varphi(p-1)$, para todo primo $p > 3$.

2.3. Construcción General De Golomb (Lempel)

Sea q potencia prima, $\mathbb{F}_q$ el campo con q elementos, α y β elementos primitivos en $\mathbb{F}_q$ (α y β generadores de $\mathbb{F}_q^*$), $a \in \mathbb{F}_q^*$, $< \alpha >= \mathbb{F}_q^*$ y $< \beta >= \mathbb{F}_q^*$.

Teorema 2.3.1. $G(q, \alpha, \beta, a) := \left\{(k, log_\beta(a - \alpha^k)) : k \in [1, q-2], \alpha^k \neq a\right\}$, *donde* $a{=}\alpha^t$, *es un conjunto de Sidon con* $q-2$ *elementos en el grupo aditivo*

$$\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} \equiv [0, q-2] \times [0, q-2].$$

Demostración. Sean $i, j, k, l \in [1, q-1], \alpha^i, \alpha^j, \alpha^k, \alpha^l$ todos distintos de a y suponga
$(i, \log_\beta(a - \alpha^i)) + (j, \log_\beta(a - \alpha^j)) = (k, \log_\beta(a - \alpha^k)) + (l, \log_\beta(a - \alpha^l))$
de donde

$$i + j = k + l \pmod{q-1}. \tag{2.3}$$

Del mismo modo

$$\log_\beta(a - \alpha^i) + \log_\beta(a - \alpha^j) \equiv \log_\beta(a - \alpha^k) + \log_\beta(a - \alpha^l) \pmod{q-1}$$
$$\log_\beta\left[(a - \alpha^i)(a - \alpha^j)\right] \equiv \log_\beta\left[(a - \alpha^k)(a - \alpha^l)\right] \pmod{q-1}$$

como $\log_\beta$ es inyectiva en $\mathbb{F}_q^*$ se satisface

$$(a - \alpha^i)(a - \alpha^j) = (a - \alpha^k)(a - \alpha^l)$$
$$a^2 - a\alpha^i - a\alpha^j + \alpha^{i+j} = a^2 - a\alpha^l - a\alpha^k + \alpha^{k+l},$$

Por (2.3) se tiene

$$\begin{aligned} \alpha^{i+j} &= \alpha^{k+l} \\ -a(\alpha^i + \alpha^j) &= -a(\alpha^k + \alpha^l) \end{aligned}$$

$$\alpha^i + \alpha^j = \alpha^k + \alpha^l \tag{2.4}$$

ya que $a \neq 0$. Por otro lado, de (2.3) se sigue

$$\alpha^i \alpha^j = \alpha^k \alpha^l. \tag{2.5}$$

en $\mathbb{F}_q^*$. De (2.4) y (2.5) por el Lema 2.1.2, $\{\alpha^i, \alpha^j\} = \left\{\alpha^k, \alpha^l\right\}$ y así $\{i, j\} = \{k, l\}$.
Por tanto $G(q, \alpha, \beta, a)$ es un conjunto de Sidon de orden $q-2$. □

Corolario 2.3.1. *$G(q, \alpha, \beta, 1)$ es un arreglo Costas de orden $q-2$.*

Demostración. Sea
$G(q, \alpha, \beta, 1) = \left\{(1, \log_\beta(1-\alpha)), (2, log_\beta(1-\alpha^2)), ..., (q-2, \log_\beta(1-\alpha^{q-2}))\right\}$,
$G(q, \alpha, \beta, 1) =$
$\left\{(1, \log_\beta(\alpha-\alpha)), (2, log_\beta(\alpha-\alpha^2)), \ldots, (q-2, \log_\beta(\alpha-\alpha^{q-2})), (q-1, \log_\beta(\alpha-\alpha^{q-1}))\right\}$. □

Ejemplo 2.3.1. *Sea $q = 3^2$ y α una raíz de $x^2 + x + 2$ y $\beta = 2\alpha + 2$. En las Tablas* 2.10 *y* 2.11 *se muestran las potencias α^k y β^k cuando k recorre todo* $[1, 8]$.

k	1	2	3	4	5	6	7	8
α^k	α	2α+1	2α+2	2	2α	α+2	α+1	1

Tabla 2.10: Potencias de la raiz α del polinomio $x^2 + x + 2$, cuando k recorre todo $[1, 8]$

k	1	2	3	4	5	6	7	8
β^k	2α+2	α+2	α	2	α+1	2α+1	2α	1

Tabla 2.11: Potencias de la raiz $\beta = 2\alpha + 2$ cuando k recorre todo $[1, 8]$

Por lo tanto $G\ (q, \alpha, \beta) = \{(1, 6), (2, 3), (3, 2), (4, 4), (5, 5), (6, 1), (7, 7)\}$ es un arreglo Costas de orden 7.

Nota 2.3.1. En la construcción de Golomb con $\alpha = \beta$ se obtiene la construcción de Lempel.

Teorema 2.3.2. *$L(q, \alpha, a) := \left\{k, \log_\alpha(a - \alpha^k) : k \in [1, q-2], \alpha^k \neq a\right\}$, donde a=α^t, es un conjunto de Sidon con $q-2$ elementos en el grupo aditivo*

$$\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1} \equiv [0, q-2] \times [0, q-2].$$

Demostración. Análoga a la construcción de Golomb con $\alpha = \beta$. □

Corolario 2.3.2. *$L(q, \alpha, 1)$ es un arreglo Costas de orden $q-2$.*

Demostración. Análoga a al Corolario 2.3.1 con $\alpha = \beta$. □

Ejemplo 2.3.2. *Sean* $q = 3^2$, α *una raíz de* $x^2 + x + 2$ *entonces* $F_q \cong F_3(\alpha)$ *y* $F_q{}^* = < 1 + \alpha >$.

En la Tabla 2.12 *se muestran las potencias* α^k *cuando* k *recorre todo* $[1, 8]$.

k	1	2	3	4	5	6	7	8
α^k	α	2α+1	2α+2	2	2α	α+2	α+1	1

Tabla 2.12: Potencias de la raiz α del polinomio $x^2 + x + 2$ cuando k recorre todo $[1, 8]$

Por lo tanto $L\ (q, \alpha) = \{(1, 2), (2, 1), (3, 6), (4, 4), (5, 7), (6, 3), (7, 5)\}$ *es un arreglo Costas de orden* 7.

Capítulo 3

Conclusiones

Este capítulo presenta las conclusiones de este trabajo.

- Los conjuntos:

  1. $W_1(p,\alpha) := \{(i,\alpha^i) : i = 1,2,...,p-1\}$
  2. $W_1^T(\alpha,p) := \{(\alpha^i,i) : i = 1,2,...,p-1\}$

  son arreglos Costas con $p-1$ elementos.

- Para todo $(u,v) \in (\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*$, los conjuntos

  1. $W_1(p,\alpha,u,v) = \{(ui, v\alpha^i) : 1 \leq i \leq p-1\} = (u,v)W_1(p,\alpha)$,
  2. $W_1^T(p,\alpha,v,u) = \{(v\alpha^i, ui) : 1 \leq i \leq p-1\} = (v,u)W_1^T(p,\alpha)$.

  son arreglos Costas con $p-1$ elementos.

- Los conjuntos

  $$W_1(\alpha) := \left\{(i,\alpha^i) : i = 1,2,....p-1\right\},$$

  $$W_1(\beta) := \left\{(i,\beta^i) : i = 1,2,....p-1\right\}$$

  están relacionados de la siguiente forma

  $$W_1(\beta) = (u,v)W_1(\alpha),$$

De la misma manera los conjuntos

$$W_1^T(\alpha) := \left\{(i, \alpha^i) : i = 1, 2, ...p-1\right\},$$

$$W_1^T(\beta) := \left\{(i, \beta^i) : i = 1, 2, ...p-1\right\},$$

están relacionados mediante

$$W_1^T(\beta) = (v, u)W_1^T(\alpha)$$

donde $(u, v) = ((\log_\alpha(\beta))^{-1}, 1) \in (\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*$.
Es decir el cambio de la raíz primitiva es equivalente a multiplicar por una unidad adecuada.

- En $(\mathbb{Z}_{p-1} \times \mathbb{Z}_p, +, \cdot)$ anillo conmutativo con unidad.
  Si $\varphi(p-1) \geq 2$, entonces $\left|(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)\right|^* = \varphi(p-1)(p-1) \geq 2(p-1) \geq 4$. Así por lo menos hay 4 unidades $(\pm 1, \pm 1)$, lo que significa que hay al menos 4 arreglos Costas.

- De unidades distintas se obtienen conjuntos distintos. Es decir

$$(u_1, v_1)W_1(\alpha) = (u_2, v_2)W_1(\alpha) \Leftrightarrow (u_1, v_1) = (u_2, v_2).$$

- Para todo primo $p > 3$ los conjuntos $W_1(p, \alpha)$ no son simétricos es decir $W \neq W^T$.

- Para todo primo p hay $\varphi(p-1)(p-1) = \left|(\mathbb{Z}_{p-1} \times \mathbb{Z}_p)^*\right|$ arreglos Costas tipo Welch de orden $p-1$.
  Similarmente hay $(p-1)\varphi(p-1) = \left|(\mathbb{Z}_p \times \mathbb{Z}_{p-1})^*\right|$ arreglos Costas tipo Welch transpuestos de orden $p-1$.

- En total hay al menos $2\varphi(p-1)(p-1)$ arreglos costas de orden $p-1$. Es decir si $\mathcal{C}(n)$ cuenta el número total de arreglos Costas de orden n, entonces $\mathcal{C}(p-1) \geq 2(p-1)\varphi(p-1)$, para todo primo $p > 3$.

- Cada permutación cíclica de las filas de un arreglo Costas tipo Welch es de nuevo un arreglo Costas de orden $p-1$.

Apéndice A

Campos Finitos

En este apéndice se presentan algunas definiciones y resultados básicos de la teoría de campos finitos necesaria para el desarrollo de este trabajo. Algunos de los resultados que se presentan no tienen su respectiva demostración, pero sus pruebas pueden ser consultadas en [7, Cap.1 y 2].

A.1. Campos Finitos Y Subcampos

Un campo finito, es un anillo con identidad $1 \neq 0$ tal que sus elementos no nulos forman un grupo abeliano bajo la multiplicación y tiene un número finito de elementos. Los campos de clases residuales $\mathbb{Z}/(p)$ son nuestros primeros ejemplos de campos finitos, esto es, de campos que contienen únicamente finitos elementos. A continuación presentamos algunos resultados básicos de la teoría de campos finitos.

Definición A.1.1. *Para un primo p, sea $\mathbb{F}_p$ el conjunto $\{0, 1, \ldots, p-1\}$ de enteros, y sea $\psi : \mathbb{Z}/(p) \to \mathbb{F}/(p)$ la aplicación definida mediante $\psi([a]) = a$, para $a = 0, 1, \ldots, p-1$. Entonces $\mathbb{F}_p$, dotado con la estructura de campo inducida por ψ, es un campo finito, llamado el campo de Galois de orden p.*

Teorema A.1.1. *Sea p un número primo y q potencia prima,*

(a) Si $\mathbb{F}$ es un campo finito con característica p,entonces $|\mathbb{F}| = p^n$, donde n es el grado de $\mathbb{F}$ sobre un subcampo primo $\mathbb{F}_p$.

(b) *Para todo entero positivo n, existe un campo finito con q^n elementos, además cualquier campo finito con q^n elementos es isomorfo al campo de descomposición de $x^{q^n} - x$, sobre $\mathbb{F}_q$.*

(c) *Si $\mathbb{F}$ es un campo finito con q elementos, entonces para todo $\alpha \in \mathbb{F}$ se cumple que $\alpha^q = \alpha$.*

Por tanto, si $\mathbb{F}$ es un campo con q elementos, donde q es una potencia prima de la característica, y $\mathbb{L}$ es una extensión finita de $\mathbb{F}$ de grado h, entonces $\mathbb{L}$ se denota por $\mathbb{F}_{q^h}$, que consiste de las raíces de $x^{q^n} - x$, sobre $\mathbb{F}_p$.
Ahora, los subcampos de un campo finito $\mathbb{F}_{q^h}$, están caracterizados por los divisores positivos de h.

Teorema A.1.2 (Criterio de subcampos). *Sea $\mathbb{F}_{q^h}$, el campo finito con q^h elementos. Entonces todo subcampo de $\mathbb{F}_{q^h}$ tiene orden q^d, donde d es un divisor positivo de h. Recíprocamente, si d es un divisor positivo de h, entonces existe exactamente un subcampo de $\mathbb{F}_{q^h}$ con q^d elementos.*

Ejemplo A.1.1. *Los subcampos de $\mathbb{F}_{5^{42}}$, están determinados por los divisores positivos de 42 y se relacionan mediante el siguiente diagrama.*

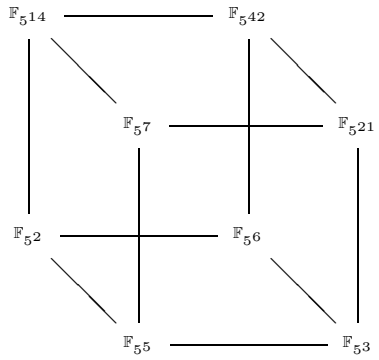


Figura A.1: Subcampos de $\mathbb{F}_{5^{42}}$.

A.2. El Grupo De Unidades De Un Campo Finito

Para un campo finito $\mathbb{F}_q$, denotamos mediante $\mathbb{F}_q^*$ al grupo multiplicativo de los elementos no nulos de $\mathbb{F}_q$. El siguiente resultado enuncia una propiedad útil de este grupo.

Teorema A.2.1. *Para todo q potencia prima, el grupo multiplicativo $\mathbb{F}_q^*$ es cíclico.*

Demostración. Asumiendo que $q \geq 3$, sea $h = q - 1 = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ la descomposición en factores primos del orden del grupo $\mathbb{F}_q^*$.
Para cada $0 \leq i \leq m$, el polinomio $x^{h/p_i} - 1$, tiene a lo mas h/p_i raíces en $\mathbb{F}_q$ y como $h/p_i < h$, se sigue que existe un elemento no nulo a_i en $\mathbb{F}_q$ que no es raíz de este polinomio. Considérese el elemento $b_i = a_i^{h/p_i^{r_i}}$. Nótese que $b_i^{p_i^{r_i}} = 1$, de esta manera el orden de b_i es un divisor de $p_i^{r_i}$ y es por tanto de la forma $p_i^{s_i}$, donde $0 \leq s_i \leq r_i$. por otro lado

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$$

y asi el orden de b_i es $p_i^{r_i}$. Para terminar, se vera que $b = b_1 b_2 \cdots b_m$ tiene orden h.
Argumentando por contradicción, supóngase que el orden de b es un divisor propio de h y de esta forma,un divisor de al menos uno de los enteros h/p_i, $1 \leq i \leq m$. Sin perdida de generalidad, supóngase que h/p_1. Entonces

$$b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1} = b^{h/p_1} = 1.$$

Ahora, si $2 \leq i \leq m$, entonces $p_i^{r_i}$ divide a h/p_1 y así $b_i^{h/p_1} = 1$. Luego $b_1^{h/p_1} = 1$, lo cual implica que el orden de b divide a h/p_1, que no es posible dado que el orden de b es $p_1^{r_1}$. por tanto, $\mathbb{F}_q^*$ es un grupo cíclico generado por b. □

Un generador del grupo cíclico $\mathbb{F}_q^*$, como b en el Teorema anterior se llama un **elemento primitivo** de $\mathbb{F}_q$. Además, un polinomio $f \in \mathbb{F}_q[x]$ de grado $m \geq 1$, se llama un **polinomio primitivo** sobre $\mathbb{F}_q$, si es el polinomio mínimal sobre $\mathbb{F}_q$ de un elemento primitivo de $\mathbb{F}_q^m$. El siguiente Teorema muestra que un elemento primitivo es también un elemento que sirve para definir a $\mathbb{F}_q$, como una extensión de uno de sus subcampos.

Teorema A.2.2. *Sean, $\mathbb{F}_q$ un campo finito y $\mathbb{F}_q^h$ una extensión finita de $\mathbb{F}_q$. Entonces $\mathbb{F}_q^h$ es una extensión simple de $\mathbb{F}_q$ y si ξ es un elemento primitivo de $\mathbb{F}_q^h$, entonces $\mathbb{F}_q^h = \mathbb{F}_q(\xi)$.*

A.3. Polinomios Sobre Un Campo Finito

Dado un polinomio $p(x)$ irreducible sobre $\mathbb{F}_q$ de grado m, es importante notar, que a diferencia de los polinomios sobre un campo de característica cero, es suficiente extender $\mathbb{F}_q$ con una raíz de $p(x)$ para obtener el campo de descomposición de $p(x)$ y sus m raíces están dadas de manera particular.

Teorema A.3.1. *Si $p(x)$ es un polinomio irreducible de grado m, sobre $\mathbb{F}_q$, entonces $p(x)$ tiene una raíz α en $\mathbb{F}_q^m$. Más aún, todas las raíces de $p(x)$ son simples y están dadas por los m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_q^m$.*

Teorema A.3.2. *Sean, $p(x)$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado n y $k \in \mathbb{N}$. Entonces $p(x)$ se descompone en d polinomios irreducibles en $\mathbb{F}_{q^k}[x]$, del mismo grado n/d, donde $d = mcd(n, k)$.*

Una consecuencia inmediata es que $p(x) \in \mathbb{F}_q[x]$, sigue siendo irreducible sobre $\mathbb{F}_{q^k}$ si y sólo si $mcd(n, k) = 1$.

Apéndice B

Lista De Arreglos Costas Tipo Welch Y Tipo Golomb

Este apéndice presenta algunos resultados importantes obtenidos en el desarrollo de este trabajo, en especial, se hizo un estudio a fondo de las construcciones de arreglos Costas tipo Welch y Golomb usando las unidades.
A continuación se describirá el proceso a seguir en las siguientes secciones

a) Dado un primo p o una potencia prima q se debe encontrar los elementos primitivos del campo determinado (Función φ Euler).

b) Aplicar la construcción a partir de los elementos primitivos, como se muestra en las Tablas B.1 a B.4, y B.9 a B.18.

c) Escoger un vector permutación generado por algún elemento primitivo y multiplicarlo por las unidades correspondientes, como se muestra en las Tablas B.5 a B.8 y B.19.

B.1. Arreglos Costas Tipo Welch En $\mathbb{Z}_{p-1} \times \mathbb{Z}_p$.

Ejemplo B.1.1. *Con $p = 11$, los elementos primitivos de $\mathbb{Z}_{11}$ son $2, 6, 7$ y 8. A continuación se aplicará la construcción de Welch para*

- $\alpha = 2$. $W_{(2)} = \{(1,2),(2,4),(3,8),(4,5),(5,10),(6,9),(7,7),(8,3),(9,6),(10,1)\}$

i	1	2	3	4	5	6	7	8	9	10
2^i(mód11)	2	4	8	5	10	9	7	3	6	1

Tabla B.1: Construcción de Welch con $p = 11$ y $\alpha = 2$.

- $\alpha = 6$. $W_{(6)} = \{(1,6),(2,3),(3,7),(4,9),(5,10),(6,5),(7,8),(8,4),(9,2),(10,1)\}$.

i	1	2	3	4	5	6	7	8	9	10
6^i(mód11)	6	3	7	9	10	5	8	4	2	1

Tabla B.2: Construcción de Welch con $p = 11$ y $\alpha = 6$.

- $\alpha = 7$. $W_{(7)} = \{(1,7),(2,5),(3,2),(4,3),(5,10),(6,4),(7,6),(8,9),(9,8),(10,1)\}$.

i	1	2	3	4	5	6	7	8	9	10
7^i(mód11)	7	5	2	3	10	4	6	9	8	1

Tabla B.3: Construcción de Welch con $p = 11$ y $\alpha = 7$.

- $\alpha = 8$. $W_{(8)} = \{(1,8),(2,9),(3,6),(4,4),(5,10),(6,3),(7,2),(8,5),(9,7),(10,1)\}$.

i	1	2	3	4	5	6	7	8	9	10
8^i(mód11)	8	9	6	4	10	3	2	5	7	1

Tabla B.4: Construcción de Welch con $p = 11$ y $\alpha = 8$.

El grupo de unidades en $\mathbb{Z}_{10} \times \mathbb{Z}_{11}$ *está determinado por*

$$U(\mathbb{Z}_{10} \times \mathbb{Z}_{11}) = \{1,3,7,9\} \times \{1,2,\ldots,10\},$$

para un total de 40 *unidades.*

	Unidad	Vector permutación
$W_{(2)} = [2, 4, 8, 5, 10, 9, 7, 3, 6, 1]$	(1,1)	$W_{(2)} = [2, 4, 8, 5, 10, 9, 7, 3, 6, 1]$
	(1,2)	$[4, 8, 5, 10, 9, 7, 3, 6, 1, 2]$
	(1,3)	$[6, 1, 2, 4, 8, 5, 10, 9, 7, 3]$
	(1,4)	$[8, 5, 10, 9, 7, 3, 6, 1, 2, 4]$
	(1,5)	$[10, 9, 7, 3, 6, 1, 2, 4, 8, 5]$
	(1,6)	$[1, 2, 4, 8, 5, 10, 9, 7, 3, 6]$
	(1,7)	$[3, 6, 1, 2, 4, 8, 5, 10, 9, 7]$
	(1,8)	$[5, 10, 9, 7, 3, 6, 1, 2, 4, 8]$
	(1,9)	$[7, 3, 6, 1, 2, 4, 8, 5, 10, 9]$
	(1,10)	$[9, 7, 3, 6, 1, 2, 4, 8, 5, 10]$
	(3,1)	$W_{(7)} = [7, 5, 2, 3, 10, 4, 6, 9, 8, 1]$
	(3,2)	$[3, 10, 4, 6, 9, 8, 1, 7, 5, 2]$
	(3,3)	$[10, 4, 6, 9, 8, 1, 7, 5, 2, 3]$
	(3,4)	$[6, 9, 8, 1, 7, 5, 2, 3, 10, 4]$
	(3,5)	$[2, 3, 10, 4, 6, 9, 8, 1, 7, 5]$
	(3,6)	$[9, 8, 1, 7, 5, 2, 3, 10, 4, 6]$
	(3,7)	$[5, 2, 3, 10, 4, 6, 9, 8, 1, 7]$
	(3,8)	$[1, 7, 5, 2, 3, 10, 4, 6, 9, 8]$
	(3,9)	$[8, 1, 7, 5, 2, 3, 10, 4, 6, 9]$
	(3,10)	$[4, 6, 9, 8, 1, 7, 5, 2, 3, 10]$
	(7,1)	$W_{(8)} = [8, 9, 6, 4, 10, 3, 2, 5, 7, 1]$
	(7,2)	$[5, 7, 1, 8, 9, 6, 4, 10, 3, 2]$
	(7,3)	$[2, 5, 7, 1, 8, 9, 6, 4, 10, 3]$
	(7,4)	$[10, 3, 2, 5, 7, 1, 8, 9, 6, 4]$
	(7,5)	$[7, 1, 8, 9, 6, 4, 10, 3, 2, 5]$
	(7,6)	$[4, 10, 3, 2, 5, 7, 1, 8, 9, 6]$
	(7,7)	$[1, 8, 9, 6, 4, 10, 3, 2, 5, 7]$
	(7,8)	$[9, 6, 4, 10, 3, 2, 5, 7, 1, 8]$
	(7,9)	$[6, 4, 10, 3, 2, 5, 7, 1, 8, 9]$
	(7,10)	$[3, 2, 5, 7, 1, 8, 9, 6, 4, 10]$

Tabla B.5: Multiplicación de un Costas tipo Welch en $\mathbb{Z}_{10} \times \mathbb{Z}_{11}$ por las unidades.

$W_{(2)} = [2,4,8,5,10,9,7,3,6,1]$	(9,1)	$W_{(6)} = [6,3,7,9,10,5,8,4,2,1]$
	(9,2)	$[1,6,3,7,9,10,5,8,4,2]$
	(9,3)	$[7,9,10,5,8,4,2,1,6,3]$
	(9,4)	$[2,1,6,3,7,9,10,5,8,4]$
	(9,5)	$[8,4,2,1,6,3,7,9,10,5]$
	(9,6)	$[3,7,9,10,5,8,4,2,1,6]$
	(9,7)	$[9,10,5,8,4,2,1,6,3,7]$
	(9,8)	$[4,2,1,6,3,7,9,10,5,8]$
	(9,9)	$[10,5,8,4,2,1,6,3,7,9]$
	(9,10)	$[5,8,4,2,1,6,3,7,9,10]$

Tabla B.6: Continuación Tabla 3.5

B.2. Arreglos Costas Tipo Welch En $\mathbb{Z}_p \times \mathbb{Z}_{p-1}$.

Ejemplo B.2.1. *Del Ejemplo B.1.1 se tiene*

$W_{(2)}^T = \{(1,10),(2,1),(3,8),(4,2),(5,4),(6,9),(7,7),(8,3),(9,6),(10,5)\}$,

$W_{(6)}^T = \{(1,10),(2,9),(3,2),(4,8),(5,6),(6,1),(7,3),(8,7),(9,4),(10,5)\}$,

$W_{(7)}^T = \{(1,10),(2,3),(3,4),(4,6),(5,2),(6,7),(7,1),(8,9),(9,8),(10,5)\}$,

$W_{(8)}^T = \{(1,10),(2,7),(3,6),(4,4),(5,8),(6,3),(7,9),(8,1),(9,2),(10,5)\}$.

El grupo de unidades en $\mathbb{Z}_{11} \times \mathbb{Z}_{10}$ *es* $U(\mathbb{Z}_{11} \times \mathbb{Z}_{10}) = \{1,2,\ldots,10\} \times \{1,3,7,9\}$ *, para un total de* 40 *unidades.*

	Unidad	Vector permutación
$W_{(2)}^T = [10,1,8,2,4,9,7,3,6,5]$	(1,1)	$W_{(2)}^T = [10,1,8,2,4,9,7,3,6,5]$
	(1,3)	$W_{(7)}^T = [10,3,4,6,2,7,1,9,8,5]$
	(1,7)	$W_{(8)}^T = [10,7,6,4,8,3,9,1,2,5]$
	(1,9)	$W_{(6)}^T = [10,9,2,8,6,1,3,7,4,5]$
	(2,1)	$[9,10,7,1,3,8,6,2,5,4]$
	(2,3)	$[7,10,1,3,9,4,8,6,5,2]$
	(2,7)	$[3,10,9,7,1,6,2,4,5,8]$
	(2,9)	$[1,10,3,9,7,2,4,8,5,6]$

Tabla B.7: Multiplicación de un Costas tipo Welch en $\mathbb{Z}_{11} \times \mathbb{Z}_{10}$ por las unidades.

$W_{(2)}^T = [10, 1, 8, 2, 4, 9, 7, 3, 6, 5]$	(3,1)	$[2, 3, 10, 4, 6, 1, 9, 5, 8, 7]$
	(3,3)	$[6, 9, 10, 2, 8, 3, 7, 5, 4, 1]$
	(3,7)	$[4, 1, 10, 8, 2, 7, 3, 5, 6, 9]$
	(3,9)	$[8, 7, 10, 6, 4, 9, 1, 5, 2, 3]$
	(4,1)	$[8, 9, 6, 10, 2, 7, 5, 1, 4, 3]$
	(4,3)	$[4, 7, 8, 10, 6, 1, 5, 3, 2, 9]$
	(4,7)	$[6, 3, 2, 10, 4, 9, 5, 7, 8, 1]$
	(4,9)	$[2, 1, 4, 10, 8, 3, 5, 9, 6, 7]$
	(5,1)	$[6, 7, 4, 8, 10, 5, 3, 9, 2, 1]$
	(5,3)	$[8, 1, 2, 4, 10, 5, 9, 7, 6, 3]$
	(5,7)	$[2, 9, 8, 6, 10, 5, 1, 3, 4, 7]$
	(5,9)	$[4, 3, 6, 2, 10, 5, 7, 1, 8, 9]$
	(6,1)	$[1, 2, 9, 7, 5, 10, 8, 4, 7, 6]$
	(6,3)	$[3, 6, 7, 9, 5, 10, 4, 2, 1, 8]$
	(6,7)	$[7, 4, 3, 1, 5, 10, 6, 8, 9, 2]$
	(6,9)	$[9, 8, 1, 3, 5, 10, 2, 6, 3, 4]$
	(7,1)	$[3, 4, 1, 5, 7, 2, 10, 6, 9, 8]$
	(7,3)	$[9, 2, 3, 5, 1, 6, 10, 8, 7, 4]$
	(7,7)	$[1, 8, 7, 5, 9, 4, 10, 2, 3, 6]$
	(7,9)	$[7, 6, 9, 5, 3, 8, 10, 4, 1, 2]$
	(8,1)	$[7, 8, 5, 9, 1, 6, 4, 10, 3, 2]$
	(8,3)	$[1, 4, 5, 7, 3, 8, 2, 10, 9, 6]$
	(8,7)	$[9, 6, 5, 3, 7, 2, 8, 10, 1, 4]$
	(8,9)	$[3, 2, 5, 1, 9, 4, 6, 10, 7, 8]$
	(9,1)	$[4, 5, 2, 6, 8, 3, 1, 7, 10, 9]$
	(9,3)	$[2, 5, 6, 8, 4, 9, 3, 1, 10, 7]$
	(9,7)	$[8, 5, 4, 2, 6, 1, 7, 9, 10, 3]$
	(9,9)	$[6, 5, 8, 4, 2, 7, 9, 3, 10, 1]$
	(10,1)	$[5, 6, 3, 7, 9, 4, 2, 8, 1, 10]$
	(10,3)	$[5, 8, 9, 1, 7, 2, 6, 4, 3, 10]$
	(10,7)	$[5, 2, 1, 9, 3, 8, 4, 6, 7, 10]$
	(10,9)	$[5, 4, 7, 3, 1, 6, 8, 2, 9, 10]$

Tabla B.8: Continuación Tabla 3.7

B.3. Arreglos Costas Tipo Golomb En $\mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1}$.

Ejemplo B.3.1. *Con $q = 11$, los elementos primitivos de $\mathbb{Z}_{11}$ son $2, 6, 7$ y 8. A continuación se aplicará la construcción de Golomb para*

- $\alpha = \beta = 2$. (Lempel)

  $G_{(2,2)} = \{(1,5),(2,3),(3,2),(4,7),(5,1),(6,8),(7,4),(8,6),(9,9)\}$

i	1	2	3	4	5	6	7	8	9	10
$2^i(\text{mód}11)$	2	4	8	5	10	9	7	3	6	1
$(1-2^i)(\text{mód}11)$	10	8	4	7	2	3	5	9	6	–
$j = \log_2(1-2^i)$	5	3	2	7	1	8	4	6	9	–

Tabla B.9: Construcción de Golomb con $q = 11$, $\alpha = \beta = 2$

- $\alpha = \beta = 6$. (Lempel)

  $G_{(6,6)} = \{(1,1),(2,4),(3,6),(4,2),(5,9),(6,3),(7,8),(8,7),(9,5)\}$

i	1	2	3	4	5	6	7	8	9	10
$6^i(\text{mód}11)$	6	3	7	9	10	5	8	4	2	1
$(1-6^i)(\text{mód}11)$	6	9	5	3	2	7	4	8	10	–
$j = \log_6(1-6^i)$	1	4	6	2	9	3	8	7	5	–

Tabla B.10: Construcción de Golomb con $q = 11$, $\alpha = \beta = 6$

- $\alpha = \beta = 7$. (Lempel)

  $G_{(7,7)} = \{(1,2),(2,1),(3,5),(4,8),(5,3),(6,9),(7,7),(8,4),(9,6)\}$

i	1	2	3	4	5	6	7	8	9	10
$7^i(\text{mód}11)$	7	5	2	3	10	4	6	9	8	1
$(1-7^i)(\text{mód}11)$	5	7	10	9	2	8	6	3	4	–
$j = \log_7(1-7^i)$	2	1	5	8	3	9	7	4	6	–

Tabla B.11: Construcción de Golomb con $q = 11$, $\alpha = \beta = 7$

- $\alpha = \beta = 8$. (Lempel)

  $G_{(8,8)} = \{(1,4),(2,6),(3,4),(4,1),(5,7),(6,2),(7,5),(8,9),(9,8)\}$

i	1	2	3	4	5	6	7	8	9	10
$8^i(\text{mód}11)$	8	9	6	4	10	3	2	5	7	1
$(1-8^i)(\text{mód}11)$	4	3	6	8	2	9	10	7	5	–
$j = \log_8(1-8^i)$	4	6	3	1	7	2	5	9	8	–

Tabla B.12: Construcción de Golomb con $q = 11$, $\alpha = \beta = 8$

- $\alpha = 2, \beta = 6$ y $\alpha = 6, \beta = 2$

  $G_{(2,6)} = \{(1,5),(2,7),(3,8),(4,3),(5,9),(6,2),(7,6),(8,4),(9,1)\}$

  $G_{(6,2)} = \{(1,9),(2,6),(3,4),(4,8),(5,1),(6,7),(7,2),(8,3),(9,5)\}$

i	1	2	3	4	5	6	7	8	9	10
$2^i(\text{mód}11)$	2	4	8	5	10	9	7	3	6	1
$6^i(\text{mód}11)$	6	3	7	9	10	5	8	4	2	1
$(1-2^i)(\text{mód}11)$	10	8	4	7	2	3	5	9	6	–
$(1-6^i)(\text{mód}11)$	6	9	5	3	2	7	4	8	10	–
$j = \log_6(1-2^i)$	5	7	8	3	9	2	6	4	1	–
$j = \log_2(1-6^i)$	9	6	4	8	1	7	2	3	5	–

Tabla B.13: Construcción de Golomb con $q = 11$, $\alpha = 2, \beta = 6$ y $\alpha = 6, \beta = 2$

- $\alpha = 2, \beta = 7$ y $\alpha = 7, \beta = 2$

  $G_{(2,7)} = \{(1,5),(2,9),(3,6),(4,1),(5,3),(6,4),(7,2),(8,8),(9,7)\}$

  $G_{(7,2)} = \{(1,4),(2,7),(3,5),(4,6),(5,1),(6,3),(7,9),(8,8),(9,2)\}$

i	1	2	3	4	5	6	7	8	9	10
$2^i(\text{mód}11)$	2	4	8	5	10	9	7	3	6	1
$7^i(\text{mód}11)$	7	5	2	3	10	4	6	9	8	1
$(1-2^i)(\text{mód}11)$	10	8	4	7	2	3	5	9	6	–
$(1-7^i)(\text{mód}11)$	5	7	10	9	2	8	6	3	4	–
$j = \log_7(1-2^i)$	5	9	6	1	3	4	2	8	7	–
$j = \log_2(1-7^i)$	4	7	5	6	1	3	9	8	2	–

Tabla B.14: Construcción de Golomb con $q = 11$, $\alpha = 2, \beta = 7$ y $\alpha = 7, \beta = 2$

- $\alpha = 2, \beta = 8$ y $\alpha = 8, \beta = 2$

  $G_{(2,8)} = \{(1,5),(2,1),(3,4),(4,9),(5,7),(6,6),(7,8),(8,2),(9,3)\}$

  $G_{(8,2)} = \{(1,2),(2,8),(3,9),(4,3),(5,1),(6,6),(7,5),(8,7),(9,4)\}$

i	1	2	3	4	5	6	7	8	9	10
$2^i(\text{mód}11)$	2	4	8	5	10	9	7	3	6	1
$8^i(\text{mód}11)$	8	9	6	4	10	3	2	5	7	1
$(1-2^i)(\text{mód}11)$	10	8	4	7	2	3	5	9	6	–
$(1-8^i)(\text{mód}11)$	4	3	6	8	2	9	10	7	5	–
$j = \log_8(1-2^i)$	5	1	4	9	7	6	8	2	3	–
$j = \log_2(1-8^i)$	2	8	9	3	1	6	5	7	4	–

Tabla B.15: Construcción de Golomb con $q = 11$, $\alpha = 2, \beta = 8$ y $\alpha = 8, \beta = 2$

- $\alpha = 6, \beta = 7$ y $\alpha = 7, \beta = 6$

  $G_{(6,7)} = \{(1,7),(2,8),(3,2),(4,4),(5,3),(6,1),(7,6),(8,9),(9,5)\}$

  $G_{(7,6)} = \{(1,6),(2,3),(3,5),(4,4),(5,9),(6,7),(7,1),(8,2),(9,8)\}$

i	1	2	3	4	5	6	7	8	9	10
$6^i(\text{mód}11)$	6	3	7	9	10	8	4	2	1	5
$7^i(\text{mód}11)$	7	5	2	3	10	4	6	9	8	1
$(1-6^i)(\text{mód}11)$	6	9	5	3	2	7	4	8	10	–
$(1-7^i)(\text{mód}11)$	5	7	10	9	2	8	6	3	4	–
$j = \log_7(1-6^i)$	7	8	2	4	3	1	6	9	5	–
$j = \log_6(1-7^i)$	6	3	5	4	9	7	1	2	8	–

Tabla B.16: Construcción de Golomb con $q = 11$, $\alpha = 6, \beta = 7$ y $\alpha = 7, \beta = 6$

- $\alpha = 6, \beta = 8$ y $\alpha = 8, \beta = 6$

  $G_{(6,8)} = \{(1,3),(2,2),(3,8),(4,6),(5,7),(6,9),(7,4),(8,1),(9,5)\}$

  $G_{(8,6)} = \{(1,8),(2,2),(3,1),(4,7),(5,9),(6,4),(7,5),(8,3),(9,6)\}$

i	1	2	3	4	5	6	7	8	9	10
$6^i(\text{mód}11)$	6	3	7	9	10	5	8	4	2	1
$8^i(\text{mód}11)$	8	9	6	4	10	3	2	5	7	1
$(1-6^i)(\text{mód}11)$	6	9	5	3	2	7	4	8	10	–
$(1-8^i)(\text{mód}11)$	4	3	6	8	2	9	10	7	5	–
$j = \log_8(1-6^i)$	3	2	8	6	7	9	4	1	5	–
$j = \log_6(1-8^i)$	8	2	1	7	9	4	5	3	6	–

Tabla B.17: Construcción de Golomb con $q = 11$, $\alpha = 6, \beta = 8$ y $\alpha = 8, \beta = 6$

- $\alpha = 7, \beta = 8$ y $\alpha = 8, \beta = 7$

  $G_{(7,8)} = \{(1,8),(2,9),(3,5),(4,2),(5,7),(6,1),(7,3),(8,6),(9,4)\}$

  $G_{(8,7)} = \{(1,6),(2,4),(3,7),(4,9),(5,3),(6,8),(7,5),(8,1),(9,2)\}$

i	1	2	3	4	5	6	7	8	9	10
$7^i(\text{mód}11)$	7	5	2	3	10	4	6	9	8	1
$8^i(\text{mód}11)$	8	9	6	4	10	3	2	5	7	1
$(1-7^i)(\text{mód}11)$	5	7	10	9	2	8	6	3	4	–
$(1-8^i)(\text{mód}11)$	4	3	6	8	2	9	10	7	5	–
$j=\log_8(1-7^i)$	8	9	5	2	7	1	3	6	4	–
$j=\log_7(1-8^i)$	6	4	7	9	3	8	5	1	2	–

Tabla B.18: Construcción de Golomb con $q=11$, $\alpha=7,\beta=8$ y $\alpha=8,\beta=7$

El grupo de unidades en $\mathbb{Z}_{10}\times\mathbb{Z}_{10}$ *es* $U(\mathbb{Z}_{10}\times\mathbb{Z}_{10})=\{1,3,7,9\}\times\{1,3,7,9\}$*, para un total de* 16 *unidades.*

	Unidad	Vector permutación $G_{(\alpha,\beta)}$
$G_{(2,2)}=[5,3,2,7,1,8,4,6,9]$	(1,1)	$G_{(2,2)}=[5,3,2,7,1,8,4,6,9]$
	(1,3)	$G_{(2,7)}=[5,9,6,1,3,4,2,8,7]$
	(1,7)	$G_{(2,8)}=[5,1,4,9,7,6,8,2,3]$
	(1,9)	$G_{(2,6)}=[5,7,8,3,9,2,6,4,1]$
	(3,1)	$G_{(7,2)}=[4,7,5,6,1,3,9,8,2]$
	(3,3)	$G_{(7,7)}=[2,1,5,8,3,9,7,4,6]$
	(3,7)	$G_{(7,8)}=[8,9,5,2,7,1,3,6,4]$
	(3,9)	$G_{(7,6)}=[6,3,5,4,9,7,1,2,8]$
	(7,1)	$G_{(8,2)}=[2,8,9,3,1,6,5,7,4]$
	(7,3)	$G_{(8,7)}=[6,4,7,9,3,8,5,1,2]$
	(7,7)	$G_{(8,8)}=[4,6,3,1,7,2,5,9,8]$
	(7,9)	$G_{(8,6)}=[8,2,1,7,9,4,5,3,6]$
	(9,1)	$G_{(6,2)}=[9,6,4,8,1,7,2,3,5]$
	(9,3)	$G_{(6,7)}=[7,8,2,4,3,1,6,9,5]$
	(9,7)	$G_{(6,8)}=[3,2,8,6,7,9,4,1,5]$
	(9,9)	$G_{(6,6)}=[1,4,6,2,9,3,8,7,5]$

Tabla B.19: Multiplicación de un Costas tipo Golomb de orden 9 por las unidades.

Apéndice C

Tabla Orden De Costas

En este apéndice se muestra el número exacto de arreglos Costas hasta $n = 29$.

C.1. Número De Arreglos Costas De Orden Dado

$\mathcal{C}(n)$ = número de arreglos Costas de orden n.

$c(n)$ = número de rotaciones y reflexiones.

$s(n)$ = número de simetrías.

n	$\mathcal{C}(n)$	$c(n)$	$s(n)$		n	$\mathcal{C}(n)$	$c(n)$	$s(n)$		n	$\mathcal{C}(n)$	$c(n)$	$s(n)$
1	1	1	—		11	4368	555	18		21	3536	446	8
2	2	1	—		12	7852	990	17		22	2052	259	5
3	4	1	1		13	12828	1616	25		23	872	114	10
4	12	2	1		14	17252	2168	23		24	200	25	0
5	40	6	2		15	19612	2467	31		25	88	12	2
6	116	17	5		16	21104	2648	20		26	56	8	2
7	200	30	10		17	18276	2294	19		27	204	29	7
8	444	60	9		18	15096	1892	10		28	712	—	—
9	760	100	10		19	10240	1283	6		29	164	—	—
10	2160	277	14		20	6464	810	4					

Tabla C.1: Total Costas, reflexiones, rotaciones y simetrías

BIBLIOGRAFÍA

[1] Costas, J. P. , *"A Study of class of detection waveforms having nearly ideal range-doopler ambiguity properties",* Proc. IEEE, Vol.72, Nº 8, pp. 996-1009, Aug. 1984.

[2] Golomb, S. W., *"IEE Transactions on Information Theory".* Vol. 53, Nº 11, November 2007.

[3] Golomb, S. W. Taylor ,H. , *"Construction and properties of Costas arrays"* . Proc. IEEE, Vol. 72, Nº 9, pp 1143-1163, Sep. 1984.

[4] Golomb, S. W. , *"Algebraic constructions for Costas arrays"*, J. Combin Theory (A.), Vol. 37, pp. 13-21, 1984.

[5] Golomb, S. W. , *" T_4 and G_4 constructions for Costas arrays"*, IEEE Trans. Inf. Theory, Vol. 38, Nº 4, pp.1404-1406, Jul. 1992.

[6] Lidl, R. Niederreiter, H. , *"Finite fields",* Encyclopedia of Mathematics and its Applications, Cambridge University Press, Vol. 20, Second edition 1997.

[7] Mollin, R. A. , *"The fundamental number theory with applications",* CRC Press, New York, 1998.

[8] Rosen, K.H. , *"Elementary number theory and its applications",* Second edition, Addison Wesley, July 1988.

[9] [Online]. Available: http://www.costasarrays.org (Visitada en Mayo de 2012.)