Involuciones de Cuerpos Finitos Obtenidos por Binomios

Dylan G. Cruz Fonseca, Andrés Ramos Rodríguez

28 de enero de 2019, Primer Semestre 2018-2019

Resumen

Las permutaciones de cuerpos finitos tienen aplicaciones en varios campos de las Matemáticas y Ciencias de Cómputos, como lo es la Criptografía. En específico, las permutaciones que son su propia inversa (involuciones) son de interés porque ofrecen una ventaja al implementarlas ya que requieren menos memoria. Estudiamos binomios de la forma $x^m(x^{\frac{q-3}{2}} + A)$ sobre $\mathbb{F}_q$ con el propósito de encontrar las condiciones en A y q tal que el binomio sea una involución. Aquí probaremos que, si $m = 1$, esta familia de binomios nunca produce permutaciones cuando de F_q donde q es potencia de un primo impar. Conjeturamos que esto es cierto para toda m.

1. Preliminares

El objetivo de esta investigación es estudiar una clase de polinomios para ver si este permuta los elementos de un cuerpo finito. Comenzaremos por definir lo que es una permutación y luego se definirá la estructura de cuerpo finito y ciertas propiedades de esta.

Definición 1. *Una **permutación** de un conjunto A es un reordenamiento de sus elementos. Podemos definir una permutación de A usando una función $f : A \to A$*

Ejemplo 1.

Sea $A = \{1, 2, 3, 4, 5\}$ y $f : A \to A$ definida por

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

donde la fila superior contiene los elementos de A y en la fila inferior están las imágenes de estos elementos bajo f. La permutación de A dada por f es $1, 3, 4, 2, 5$.

Note que para que f sea una permutación de A, f tiene que ser $1-1$ y sobre. En caso de que A sea finito, basta que cumpla con una de esas propiedades como indica la siguiente proposición.

Proposición 1. *Sea A un conjunto finito. Entonces una función $f : A \to A$ es $1-1$ si y solo si f es sobre.*

Demostración. Suponga que f es 1-1. Entonces para $a, b \in A$ tal que $a \neq b$, $f(a) \neq f(b)$. Como A es finito, f es sobre porque si no lo fuera, existiría un $c \in A$ tal que $f(a) \neq c \ \forall a \in A$. Esto implíca que existe un valor a' tal que $f(a) = a' = f(b)$ con $a \neq b$. Esto contradice la hipótesis.

Solo queda demostrarlo de la otra dirección. □

Ejemplo 2.

Sea $A = \{1, 2, 3, 4, 5\}$ y $g : A \to A$ definida por

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

Note que g no es una permutación de A ya que g no es una biyección.

Estaremos estudiando permutaciones de conjuntos que tienen estructura de cuerpo finito, le llamamos permutaciones de cuerpos finitos.

Definición 2. *Un **cuerpo finito** F_q es una estructura algebraica que consiste en un conjunto finito A, de cardinalidad q, donde $q = p^r$ con p primo y $r \in \mathbb{N}$, con las operaciones $+$ y $*$ que satisfacen los siguientes axiomas:*

- *El conjunto debe ser **cerrado** bajo ambas operaciones. Esto es, si $a, b \in F_q$, $a + b \in F_q$ y $a * b \in F_q$.*
- *El conjunto debe ser **asociativo** bajo ambas operaciones. Esto es $(a + b) + c = a + (b + c)$ y $(a * b) * c = a * (b * c) \ \forall \ a, b, c \in \mathbb{F}_q$.*

- *Ambas operaciones* ***conmutan*** *en el conjunto. Esto es, si* $a, b \in F_q$, *entonces* $a + b = b + a$ *y* $a * b = b * a$.
- *El conjunto posee* ***identidad*** *bajo ambas operaciones. Esto es,* $0 \in F_q$ *con* $0 + a = a, \forall a \in F_q$ *y* $1 \in F_q$ *con* $1 * a = a, \ \forall a \in F_q$.
- *Todos los elementos en el conjunto poseen* ***inversa aditiva*** *y todo elemento distinto de 0, posee* ***inversa multiplicativa****. Esto es,* $\forall a \in F_q \ \exists \ -a$ *tal que* $a + -a = 0$ *y* $\forall a \neq 0 \in F_q, \ \exists \ a^{-1}$ *tal que* $a * a^{-1} = 1$
- *La operación* $*$ ***distribuye*** $a +$. *Esto es,* $\forall \ a, b, c \in F_q, \ a * (b + c) = (a * b) + (a * c)$

Nota que $< \mathbb{F}_q, + >$ es un grupo y $< \mathbb{F}_q^*, * >$ es un grupo

Teorema 1. *(Teorema Pequeño de Fermat) Sea* $a \in \mathbb{F}_q$, *entonces* $a^{q-1} = 1$

A partir de ese teorema tenemos el próximo lema.

Lema 1. *Sea* $a \in \mathbb{F}_q^*$. *Entonces* $a^{\frac{q-1}{2}} = \pm 1$

Demostración. Por el Teorema 1 sabemos que $x^{q-1} = 1$. Note que eso es igual a

$$x^{q-1} - 1 = 0$$
$$\leftrightarrow (a^{\frac{q-1}{2}})^2 - 1 = 0$$
$$\leftrightarrow (a^{\frac{q-1}{2}} - 1)(a^{\frac{q-1}{2}} + 1) = 0$$

entonces $a^{\frac{q-1}{2}} = 1$ o $a^{\frac{q-1}{2}} = -1$ □

Nos interesan permutaciones de cuerpos finitos generados por polinomios.

Definición 3. *Un polinomio* $p \in \mathbb{F}_q[x]$ *se dice que es un polinomio de permutación si* $p : \mathbb{F}_q \to \mathbb{F}_q$ *define una permutación.*

Al ser esta una investigación sobre polinomios de permutación sobre cuerpos finitos, los elementos que se evalúan en el polinomio son los elementos del cuerpo.

La próxima definición es una característica importante de los cuerpos finitos y es lo que usamos para probar los resultados de esta investigación.

Definición 4. *Se dice que $\alpha \in \mathbb{F}_q$ es una* ***raíz primitiva*** *de $\mathbb{F}_q$ si α genera a $\mathbb{F}_q \setminus 0 = \mathbb{F}_q^*$. Es decir $< \alpha >= \{\alpha^0, \alpha^1, \alpha^3, ..., \alpha^{q-2}\} = \mathbb{F}_q^*$. Esto es, $< \mathbb{F}_q^*, * >$ es un grupo cíclico generado por α.*

Proposición 2. *Todo cuerpo finito $\mathbb{F}_q$ tiene raices primitivas.*

Lema 2. *Sea α una raiz primitiva de un cuerpo $\mathbb{F}_q$. Entonces $\alpha^{\frac{q-1}{2}} = -1$.*

Demostración. Por Lema 1 sabemos que para $x \in \mathbb{F}_q$, $x^{\frac{q-1}{2}} = 1$ o $x^{\frac{q-1}{2}} = -1$. Suponga que α es un raíz primitiva de $\mathbb{F}_q$. Ahora vamos a suponer que $\alpha^{\frac{q-1}{2}} = 1$. Esto implíca que $< \alpha >= \{\alpha^0, \alpha^1, \ldots, \alpha^{\frac{q-3}{2}}, \alpha^{\frac{q-1}{2}}\} = \{1, \alpha^1, \ldots, \alpha^{\frac{q-3}{2}}, 1\}$. Por definición de raíz primitiva, $< \alpha >$ tiene que generar $\mathbb{F}_q^*$ y se puede ver que $\{1, \alpha^1, \ldots, \alpha^{\frac{q-3}{2}}, 1\}$ no genera F_q^* por lo tanto llegamos a una contradicción y concluímos que $\alpha^{\frac{q-1}{2}} = -1$. □

El siguiente teorema nos ofrece un criterio par polinomio de permutación que es particularmente útil para demostrar cuando un polinomio no es de permutación.

Teorema 2. *(Criterio de Hermite) Un polinomio $P \in \mathbb{F}_q[x]$ es un polinomio de permutacion si y solo si:*

1. *P solo tiene una raíz en $\mathbb{F}_q$, y*
2. *Para todo t, $1 \leq t \leq q-2, t \not\equiv 0 \pmod{p}$, la reducción de $P(x)^t \pmod{x^q - x}$ tiene grado $\leq q-2$.*

2. Revisión de Literatura

Los polinomios de permutación sobre cuerpos finitos han sido objeto de estudio por muchos años. La siguiente tabla es una revisión de literatura que contiene los resultados de polinomios de permutación y polinomios que no son de permutación. También se hace un estudio comparativo entre estas. La ultima columna se refiere a que otros resultados de la tabla usan funciones de la misma forma.

Núm.	Polinomio	Resultado	Autor	Año	Teorema, Página y Cita	Problema Nuestro	De la forma:
1	$f(x) \in \mathbb{F}_q$	Sea $\mathbb{F}_q$ de característica p,$f(x)$ sera Polinomio de Permutación si y solo si: 1. f posee solo una raiz en $\mathbb{F}_q$. 2. Para todo entero t tal que $1 \leq t \leq q-2$ con $t \not\equiv 0$ (mód p), la reducción de $f(x)^t$ (mód $()x^q - x$) es de grado $\leq q-2$	R. Lidl		Teorema 7.4 (Hermite's Criterion), pág. 349, [6]		
2	$f(x) = x^m + ax^n \in \mathbb{F}_p$	Sea $f(x)$ un polinomio de permutación y $p > 5$, con $m > n > 0$, $a \in \mathbb{F}_p$ entonces $(m-n, p-1) \notin 2, 4$	A. Masuda	2007	Teorema 1.1, pág 1, [7]	Lillian, Dylan/ Andrés, Fermín	1
3	$f(x) = x^m + ax^n \in \mathbb{F}_p$	Sea $f(x)$ un polinomio de permutación y $p > 5$, con $m > n > 0$, $a \in \mathbb{F}_p^*$ entonces $q \leq (m-2)^4 + 4m - 4$ o $m = np^i$	A. Masuda	2009	Teorema 1.1, pág. 4169, [8]	Lillian, Dylan/ Andres, Fermín	1,2
4	$f(x) = x^m + ax^n \in \mathbb{F}_p$	Sea $f(x)$ un polinomio de permutación, con $m > n > 0$, $a \in \mathbb{F}_p^*$ entonces $p-1 \leq (m-1) * max(n, gcd(m-n, p-1))$	A. Masuda	2009	Teorema 1.2 pág. 4169, [8]	Lillian, Dylan/ Andres, Fermín	1,2,3

Núm.	Polinomio	Resultado	Autor	Año	Teorema, Página y Cita	Problema Nuestro	De la forma:
5	$x^k + ax$	Sea $1 < k < q$, k no es potencia de p, $q = p^m$, $q \geq (k^2 - 4k + 6)^2 \longrightarrow$ el polinomio no es de permutación.	D. Wan	1984	Niederreter Robinson Theorem, pág 1 [3]	Lillian, Dylan/ Andres, Fermín	2,3,4
6	$x^k + ax$	Si $1 < k < p$ con $p - 1 > (k - 1, p - 1) * (k - 1)$ y $a \neq 0$ entonces el polinomio no es de permutación	D. Wan	1984	Teorema 1.3, pág 1[3]	Lillian, Dylan/ Andres, Fermín	1,2,3,4,5
7	$x^{m+1} + ax \in \mathbb{F}_q$	Sea $q = 3m + 1$ con $a \in \mathbb{F}_q \longrightarrow$ el polinomio es de permutación	L. Carlitz	1961	Teorema 1, pág 2 [1]		1,2,3
8	$P(x) = x^m * f(x^{\frac{q-1}{d}})$						
9	$x^{m+1} + ax \in \mathbb{F}_q^r$	Sea $q \geq 7$ y $q = 2m + 1$ con $a = \frac{c^2+1}{c^2-1}, c^2 \neq \pm 1$ El polinomio es de permutación si: $q \geq 7$ El polinomio NO es de permutación si: $r > 1$	L. Carlitz	1961	Teorema 1 , pág 2[1]		1,2,3,4,5
10	$x^{\frac{q-1}{3}+1} + ax \in \mathbb{F}_{q^r}$	Sea $r \geq 2$, $p \neq 2$, $q \equiv 1$ (mód 3), $a \neq 0 \longrightarrow$ el polinomio no es de permutación.	D. Wan	1984	Teorema 1.1, pág 1 [3]		1,2,3,4,5,8

Núm.	Polinomio	Resultado	Autor	Año	Teorema, Página y Cita	Problema Nuestro	De la forma:
11	$x^{\frac{q-1}{3}+1} + ax \in \mathbb{F}_{q^r}$	Sea $r \geq 2$, $q \equiv 1 \pmod 3$, $a \neq 0 \longrightarrow$ el polinomio no es de permutación	D. Wan	1994	Teorema 1.1, pág 32[4]		1,2,3,4,5,8
12	$x^{m+\frac{q-1}{2}} + ax^m$	Sea q impar, $m \neq 0 \in \mathbb{Z}$ es polinomio de permutación si: 1. Sea $(m, q-1) = 1$. Es PP $\leftrightarrow$ $\eta(a^2-1) = 1$ 2. Sea $(m, q-1) = 2$. Es PP $\leftrightarrow$ $\eta(a^2-1) = 1$ y $q \equiv -1 \pmod 4$ y no es polinomio de permutación si: 1. $(m, q-1) \geq 3$	D. Wan	1994	Teorema 4.1, pág.34[4]	Lillian	1,2,3,4,5,8
13	$P(x) = x^m(x^{\frac{q-1}{2}} + a) \in \mathbb{F}_q$	Sea $(m, q-1) = 2$ y $q = 4k+3$, $k\mathbb{Z}$. Si $\eta(a^2-1) = -1$y $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ y $(a+1)^{m+1} = (a+1)^{\frac{q-1}{2}} = 1$ y $(a-1)^(m+1) = -1$, entonces $P(x)$ es **involución** en $\mathbb{F}_q$.	L. Gonzaléz	2018	Propocisión 3.2.3, pág 10[5]	Lillian	1,2,3,4,5,8

Núm.	Polinomio	Resultado	Autor	Año	Teorema, Página y Cita	Problema Nuestro	De la forma:
14	$P(x) = x^{q-2} + ax^{\frac{q-3}{2}} \in \mathbb{F}_q$	Sea $a \neq 0$ entonces $P(x)$ es una involución, si y solo si: 1. $q = 4k+1$ y $\eta(a+1) = \eta(a-1) = 1$ 2. $q = 4k+3$ y $\eta(a+1) = \eta(a-1) = -1$	L. Gonzaléz	2018	Proposición 3.2.2, pág 8 [5]	Lillian	1,2,3,4,5,8
15	$P(x) = x^m(x^{\frac{q-1}{2}}+a) \in \mathbb{F}_q$	Sea $P(x)$ una involución, entonces $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.	L. Gonzaléz	2018	Lema 3.2.1, pág 7[5]	Lillian	1,2,3,4,5,8
16	$P(x) = x^{\frac{q-1}{2}} + ax \in \mathbb{F}_q$	Sea q una potencia de algún primo $p \longrightarrow P(x)$ no es PP.	A. Ramos & D. Cruz	2018		Dylan/ Andreś	1,2,3,4,5,8

3. Trabajo Realizado

En este trabajo se estudiaron los polinomios de la forma

$$P(x) = x^m(x^{\frac{q-3}{2}} + A) = (x^{\frac{q-1}{2}})(x^{m-1}) + Ax^m \tag{1}$$

sobre cuerpos finitos F_q. En la primera sección se presentan los resultados obtenidos con $m = 1$. Esta es una forma más específica del binomio. Luego se presentan los resultados obtenidos al estudiar el binomio en forma general.

3.1. Forma Especfica

Se comenzó estudiando el binomio en la forma

$$P(x) = x(x^{\frac{q-3}{2}} + A) = x^{\frac{q-1}{2}} + Ax \tag{2}$$

sobre un cuerpo finito $\mathbb{F}_q$ y $A \neq 0$. Lo primero que se debe notar es que $P(0) = 0$. El resto de los valores van a ser de la forma $P(\alpha^i)$ donde α es una raíz primitiva de $\mathbb{F}_q$. También, como $A \neq 0$, $A = \alpha^k$ para $0 \leq k < q-1$. Esto es

$$P(\alpha^i) = (\alpha^i)^{\frac{q-1}{2}} + \alpha^k\alpha^i = (\alpha^{\frac{q-1}{2}})^i + \alpha^{k+i},$$

y por el Lema 2, tenemos

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

Como lo que queríamos era determinar si (2) produce permutaciones sobre $\mathbb{F}_q$, comenzamos calculando ejemplos para distintos $\mathbb{F}_q$, con $q = p$. Se hizo un programa en SageMath que evaluaba todos elementos de F_q, en $P(x)$ para todo $A \in F_p^*$ y así determinar si los permutaba. Al verificar todos los primos hasta el 41, y luego intentar algunos primos aleatorios mayores de 2 dígitos y notar que ninguno producía permutación conjeturamos que $P(x)$ nunca produce permutación.

Para demostrar que (2) nunca produce permutación sobre $\mathbb{F}_q$ demostramos que $P(x)$ no es $1-1$. Para lograr esto consideramos cuatro casos. Los primeros dos son cuando $q = 4h+1$ con $A = \alpha^k$ y k impar y par. Los otros dos son cuando $q = 4h+3$ con k impar y par. La siguiente proposición provee resultados para los primeros tres casos.

Proposición 3. *$P(x) = x(x^{\frac{q-3}{2}} + A)$ no es un polinomio de permutación en $\mathbb{F}_q$ si:*

(a) $q = 4h+1$, *donde* $q = p^r$ *con* $r \in \mathbb{N}$

(b) $q = 4h+3$, *donde* $q = p^r$ *con* $r \in \mathbb{N}$ *y* $A = \alpha^k$ *con* k *impar*

Demostración.

(a) Sea $q = 4h+1$ y k impar. Entonces evalúe α^{q-1-k} en P. Note que $q-i-k$ es impar y

$$P(\alpha^{q-1-k}) = (-1)^{q-1-k} + \alpha^{k+q-1-k} = -1 + \alpha^{q-1} = -1+1 = 0 = P(0).$$

Como $\alpha^{q-1-k} \neq 0$ tenemos que P no es $1-1$ en este caso.

Ahora supongamos que k es *par*. Entonces, $\frac{q-1}{2} - k$ es par y

$$P(\alpha^{\frac{q-1}{2}-k}) = (-1)^{\frac{q-1}{2}-k} + \alpha^{k+\frac{q-1}{2}-k} = (-1)^{\frac{q-1}{2}-k} + \alpha^{\frac{q-1}{2}} = 1+(-1) = 0 = P(0).$$

Como $\alpha^{\frac{q-1}{2}-k} \neq 0$, tenemos que P no es $1-1$ en este caso.

Con estos dos casos demostrados, se prueba que (2) no es polinomio de permutación cuando $q = 4h+1$.

(b) Sea $q = 4h+3$ y k impar. Entonces evalúe α^{2h+1-k} en P. Note que $2h+1-k$ es par y

$$P(\alpha^{2h+1-k}) = (-1)^{2h+1-k} + \alpha^{k+2h+1-k} = 1 + \alpha^{2h+1} = 1 + \alpha^{\frac{4h+2}{2}}$$

$$= 1 + \alpha^{\frac{4h+2+1-1}{2}} = 1 + \alpha^{\frac{4h+3-1}{2}} = 1 + \alpha^{\frac{q-1}{2}} = 1 - 1 = 0 = P(0)$$

y como $\alpha^{2h+1-k} \neq 0$, P no es $1-1$ para este caso.

□

Con esto ya demostrado, solo nos falta demostrar el caso en que $q = 4h+3$ y k es par. Los siguientes resultados nos ayudarían en la demostración.

Lema 3. *Si* $P(\alpha^i) = P(\alpha^j)$ *con* $i \not\equiv j \pmod{q-1}$, *entonces* $i \not\equiv j \pmod 2$

Demostración. (Por contradicción)
Suponga que $i \not\equiv j \pmod{q-1}$, $P(\alpha^i) = P(\alpha^j)$ y $i \not\equiv j \pmod 2$.
Caso 1) i, j ambos son impares:

Entonces

$$P(\alpha^i) = P(\alpha^j) \iff -1 + \alpha^{k+i} = -1 + \alpha^{k+j} \iff \alpha^{k+i} = \alpha^{k+j}$$

$$\iff \alpha^i = \alpha^j \iff i \equiv j \pmod{q-1}$$

Esto es una contradicción.
Caso 2) i, j ambos son pares:
Entonces

$$P(\alpha^i) = P(\alpha^j) \iff 1 + \alpha^{k+i} = 1 + \alpha^{k+j} \iff \alpha^{k+i} = \alpha^{k+j}$$

$$\iff \alpha^i = \alpha^j \iff i \equiv j \pmod{q-1}$$

Esto también es una contradicción. Por lo tanto, $P(\alpha^i) = P(\alpha^j)$ con $i \not\equiv j \pmod{q-1}$ implica que $i \not\equiv j \pmod 2$. □

Corolario 1. *Si $P(\alpha^i) = P(\alpha^j)$ con $i \not\equiv j$, entonces $\alpha^i \neq \alpha^j$.*

Para demostrar que P no es 1-1, necesitamos demostrar que $P(a) = P(b)$ para algún $a \neq b$

Lema 4. *Suponga que $i \neq j$, entonces $P(\alpha^i) = P(\alpha^j)$, si y solo si $\alpha^j = \alpha^i + 2\alpha^{-k}$ donde $\alpha^k = A$*

Demostración. Por Lema 3, $P(\alpha^i) = P(\alpha^j) \iff i \neq j \pmod 2$, así que vamos a suponer que i es par y j es impar. Entonces,

$$(-1)^i + \alpha^{k+i} = (-1)^j + \alpha^{j+k} \iff 1 + \alpha^{i+k} = -1 + \alpha^{j+k}$$
$$\iff 2 + \alpha^{i+k} = \alpha^{j+k} \iff 2 + \alpha^i\alpha^k = \alpha^j\alpha^k \iff$$
$$2\alpha^{-k} + \alpha^i = \alpha^j \tag{3}$$

□

Ahora lo que queremos demostrar es que siempre existen i, j tales que $\alpha^i = \alpha^j + 2$. Si demostramos esto, P no es $1-1$ y por tanto no es un polinomio de permutación. Pero antes de eso vamos a simplificar el problema con la proxima proposición.

Proposición 4. *Si $P_1(x) = x^{\frac{q-1}{2}} + x$ no es polinomio de permutación, entonces $P_2(x) = x^{\frac{q-1}{2}} + \alpha^{2s}x$*

Demostración. Si P_1 no es polinomio de permutación entonces $\exists a \neq b$ con $P_1(a) = P_1(b)$
Caso 1):

Si $a = 0$ y $b = \alpha^i$ con $P_1(a) = P_1(b)$, entonces $0 = (-1)^i + \alpha^i = (-1)^{i-2s} + \alpha^i = P_2(\alpha^{i-2s})$. Como $P_2(0) = 0$ y $\alpha^{i-2s} \neq 0$, tenemos que P_2 no es de permutación.
Caso2):

Si $a = \alpha^i \neq \alpha^j = b$ con $P_1(\alpha^i) = P_1(\alpha^j)$, entonces $P_2(\alpha^{i-2s}) = (-1)^{i-2s} + \alpha^{2s}\alpha^{i-2s} = (-1)^i + \alpha^i = (-1)^j + \alpha^j = (-1)^{j-2s} + \alpha^{2s}\alpha^{j-2s} = P_2(\alpha^{j-2s})$.

Como $\alpha^i \neq \alpha^j$, tenemos que $\alpha^i\alpha^{-2s} \neq \alpha^j\alpha^{-2s}$ y $\alpha^{i-2s} \neq \alpha^{j-2s}$. Por lo tanto P_2 no es polinomio de permutación. □

Proposición 5. *Sea $p = 4r+3, p \neq 3, 7$ para algún $f, s \in \mathbb{Z}$, $2+\alpha^{2f} = \alpha^{2s+1}$.*

Demostración. (Por contradicción)

En [2] se prueba que para todo $p \neq 2, 3, 7$ existen raíces primitivas de ambas paridades. Por lo tanto podemos asumir que α es impar.

Suponga que para todo $f \in \mathbb{Z}, 2 + \alpha^{2f} = \alpha^{2h}$ para algún h o $2 + \alpha^{2f} = 0$.

Como $p - 1$ es par,

$$3 = 2 + \alpha^{p-1} = \alpha^{2h_1} \ o \ 3 = 0$$

Esto implica que

$$5 = 2 + 3 = 2 + \alpha^{2h_1} = \alpha^{2h_2} \ o \ 5 = 0$$

De manera similar, como $1 = \alpha^{p-1} = \alpha^{4r+2}$, $1, 3, 5, ..., p - 2$ aon distintos de 0 y por lo tanto potencias pares de α.

Por lo tanto, cada impar es una potencia par de α y hay $\frac{p-1}{2}$ de ellas. En particular si α es impar, $\alpha = \alpha^{2h}$ para $0 \leq h < \frac{p-1}{2}$. Pero esto es una contradicción porque $0 \leq 2h < p - 1$ implica que $1 \not\equiv 2h$ (mód $p - 1$) y $\alpha^1 \neq \alpha^{2h}$

□

Con estos dos resultados podemos probar la próxima proposición.

Proposición 6. *Para $q = p$, $P(x) = x(x^{\frac{q-3}{2}} + A)$ nunca es un polinomio de permutación en $\mathbb{F}_q$ con*

Demostración. Para $p = 2, 3, 7$ podemos encontrar $a \neq b$ con $P(a) = P(b)$.

Los casos $p = 4h + 1, p = 4h + 3$ con $A = \alpha^k$ k impar están demostrados en la propcision 3.

Supongamos que $p = 4h + 3, A = \alpha^k$ con k par. Entonces, por la proposición 4, solo hay que demostrar que $P(x) = x^{\frac{q-1}{2}} + x$ no es polinomio de permutación.

Considere α^i y $\alpha^j = 2 + \alpha^i$ donde i es par y j es impar. Note que α^j existe por la proposición 5 y $\alpha^i \neq \alpha^j$

Tenemos que

$$\alpha^j = 2 + \alpha^i \iff -1 + \alpha^j = 1 + \alpha^i$$

$$\iff (-1)^j + \alpha^j = (-1)i + \alpha^i$$

$$\iff P(\alpha^i) = P(\alpha^j)$$

Por lo tanto, existe $\alpha^i \neq \alpha^j$ con $P(\alpha^i) = P(\alpha^j)$ y P no es 1-1. □

Este resultado tiene la limitación de que solo funciona para cuerpos F_p donde p es primo. La siguiente proposición demuestra que P no permuta para ningun cuerpo F_q.

Proposición 7. *El polinomio $P(x) = x(x^{\frac{q-3}{2}} + A)$ nunca permuta sobre $\mathbb{F}_q$.*

Demostración. Esta demostración es utilizando el Criterio de Hermite (Teorema 2). Note que podemos escribir $P(x)$ de la forma

$$P(x) = x^{\frac{q-1}{2}} + Ax$$

entonces si tomamos

$$P(x)^2 = x^{q-1} + 2Ax^{\frac{q+1}{2}} + A^2x^2$$

Por el teorema 2 nunca va a permutar, ya que $deg(P(x)^2) = q - 1$. □

Con estos resultados demostramos que P nunca permuta. Ahora estudiaremos una forma más general de P.

3.2. Forma General

En esta sección presentaremos resultados para el binomio en forma general. Es decir de la forma $x^m(x^{\frac{q-3}{2}} + A)$ donde $m > 1$ y $A \neq 0$. Muy parecido a la Proposición 3 tenemos el siguiente resultado pero en forma general.

Proposición 8. *$P(x) = x^m(x^{\frac{q-3}{2}} + A)$ no es polinomio de permutación en F_q si,*

(a) $A = \alpha^k$ con k impar donde $q = p^r$ con $r \in \mathbb{N}$

(b) $A = \alpha^k$ con k par y $q = 4h + 1$ donde $q = p^r$ con $r \in \mathbb{N}$

Demostración. Primero, observe que

$$P(x) = x^m(x^{\frac{q-3}{2}}+A) = x^{\frac{q-3+2m}{2}}+Ax^m = x^{\frac{q-1}{2}+\frac{2m-2}{2}}+Ax^m = (x^{\frac{q-1}{2}})(x^{m-1})+Ax^m$$

(a) Sea $A = \alpha^k$ con k impar. Entonces $A^{-1} = \alpha^{-k}$ con $-k$ impar. Note que

$$P(A^{-1}) = (A^{-1})^{\frac{q-1}{2}}(A^{-1})^{m-1}+A(A^{-1})^m = ((\alpha^{-k})^{\frac{q-1}{2}})(A^{-m+1})+A^{-m+1}$$

$$= (-1)^{-k}(A^{-m+1}) + A^{-m+1} = -A^{-m+1} + A^{-m+1} = 0 = P(0)$$

Como $A^{-1} \neq 0$, P no es un polinomio de permutación cuando $A = \alpha^k$ con k impar.

(b) Sea $A = \alpha^k$ con k par y $q = 4h + 1$. Entonces $A^{-1} = \alpha^{-k}$ con $-k$ par. Note que

$$P(-A^{-1}) = (-A^{-1})^{\frac{q-1}{2}}(-A^{-1})^{m-1} + A(-A^{-1})^m$$

$$= (-\alpha^{-k})^{\frac{q-1}{2}}(-A^{-1})^{m-1} + A(-A^{-1})^m$$

$$= (\alpha^{\frac{q-1}{2}})^{-k}(-1)^{m-1}(A^{-1})^{m-1} + A(A^{-1})(A^{-1})^{m-1}(-1)^m$$

$$= (-1)^{m-1}(A^{-1})^{m-1} + (A^{-1})^{m-1}(-1)^m$$

$$= (A^{-1})^{m-1}[(-1)^{m-1} + (-1)^m] = 0 = P(0)$$

Como $-A^{-1} \neq 0$, P no es polinomio de permutación caundo $A = \alpha^k$ con k impar y $q = 4h + 3$.

□

El caso que nos sobra es cuando $q = 4h + 3$ y $A = \alpha^k$. Esto es igual que en la forma específica. Por ende tenemos la próxima conjetura.

Conjetura 1.

$P(x) = x^m(x^{\frac{q-3}{2}} + A)$ no es polinomio de permutación en F_q si $q = 4h+3$ y $A = \alpha^k$ con k impar.

Para los tres casos que se demuestran, se utilizan dos valores que hacen que el polinomio nunca permute. Para el caso $q = 4h + 3$ con k par, esto no se logra. Los siguientes dos resultados nos dan dos valores que cuando los evalas en el polinomio en forma específica, nunca permutá. Esto nos proveé un punto de partida para poder demostrar que el polinomio en forma general nunca permuta.

Proposición 9. *Existe un $c \in F_q^*$ tal que $\eta(c-1) = 1$ y $\eta(c+1) = -1$.*

Demostración. Suponga que no existe c tal que $\eta(c-1) = 1$ y $\eta(c+1) = -1$. Esto implica que $\forall\ c \in F_q^*$ se cumple una de las siguientes:

- $\eta(c-1) = 1$ y $\eta(c+1) = 1$.
- $\eta(c-1) = -1$ y $\eta(c+1) = -1$.
- $\eta(c-1) = -1$ y $\eta(c+1) = 1$.

Las primeras dos llevan a contradicciones ya que la primera implica que todos los elementos de F_q son residuos cuadráticos y la segunda implica que ningún elemento de F_q es residuo cuadrático.

Para el tercer caso note que si tomas $b = c + 2$, la hipótesis nos dice que $\eta(b-1) = -1$ y $\eta(b+1) = 1$, pero $\eta(b-1) = \eta(c+1)$ lo cual implica que $-1 = 1$. Por lo tanto llegamos a una contradicción. □

Proposición 10. *El polinomio $P(x) = x^{\frac{q-1}{2}} + Ax$ no es PP cuando $q = 4h+3$ y $A = \alpha^k$ con k par.*

Demostración. Sea $c \in F_q^*$ tal que $\eta(c^2-1) = -1$ y $\eta(c+1) = -1, \eta(c-1) = 1$. Note que

$$P(c+1) = (c+1)^{\frac{q-1}{2}} + (c+1) = -1 + c + 1 = c = 1 + c - 1 = (c-1)^{\frac{q-1}{2}} + (c-1) = P(c-1)$$

Como $c + 1 \neq c - 1$, P no es PP. □

4. Trabajo Futuro

- Demotrar que $x^m(x^{\frac{q-3}{2}} + A)$ no permuta cuando $q = 4h + 3$ y $A = \alpha^k$ con k par

5. Congresos

6. Presentaciones

- Presentación de poster en el Seminario Interuniversitario de Investigacin en Ciencias Matemticas (SIDIM) XXXIII. (24 de marzo de 2018)
- Presentación oral en el Junior Technical Meeting (JTM)/Puerto Rico Interdisciplinary Scientific Meeting (PRISM). (28 de abril de 2018)

Referencias

[1] Leonard Carlitz. Some theorems on permutation polynomials. *Bull. Amer. Math. Soc.*, 68(2):120–122, 03 1961.

[2] Stephen D. Cohen and Tim Trudgian. Lehmer numbers and primitive roots modulo a prime. 2(1):1–11, 2017.

[3] Wan Daqing. Permutation polynomials over finite fields. *Acta Mathematica Sinica, New Series*, 3, 1984.

[4] Wan Daqing. Permutation binomials over finite fields. *Acta Mathematica Sinica, New Series*, 10, 01 1994.

[5] Lillian González. Involuciones de Cuerpos Finitos obtenidos por Binomios. Technical Report 1, 2018.

[6] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2nd edition, 1996.

[7] Ariane Masuda and Michael Zieve. Nonexistence of permutation binomials of certain shapes. *Electronic Journal of Combinatorics*, 14, 08 2007.

[8] Ariane Masuda and Michael Zieve. *Transactions of the American Mathematical Society*, 361(8), 2009.