Sumas de Monomios de Permutación

Karla Borges, Javier Santiago

Mayo 2019

Resumen

Las permutaciones juegan un papel importante en las comunicaciones, ya que se utilizan en una variedad de aplicaciones, desde la teoría de códigos hasta la criptografía. Los polinomios que generan permutaciones se llaman polinomios de permutación. Nosotros estudiamos binomios de la forma $f(x) = x^m + Ax^n = x^n(x^{m-n} + A)$ sobre cuerpos finitos $\mathbb{F}_p$, donde x^m y Ax^n son también monomios de permutación. El objetivo es encontrar las condiciones para que $f(x)$ permute $\mathbb{F}_p$. Aquí demostramos que $f(x)$ nunca es polinomio de permutación para $\mathbb{F}_q$, donde $q = 2p+1$, p primo, y conjeturamos que si $x^n(x^{m-n} + A)$ es un polinomio de permutación, donde $m - n = \frac{p-1}{d}$, entonces $A^d + (-1)^{d+1}$ es un residuo edésimo.

1. Introducción

Sea $q = p^r$ donde p es primo. Se denota $\mathbb{F}_q$ para denotar el cuerpo finito de q elementos, y $\mathbb{F}_q^*$ para denotar $\mathbb{F}_q/\{0\}$.

El objetivo de nuestra investigación es construir polinomios que permutan los elementos de un cuerpo finito. Monomios que permutan los elementos de $\mathbb{F}_q$ ya han sido caracterizados, donde un monomio de grado n permuta $\mathbb{F}_q$ sí y solo sí n es relativamente primo con $q - 1$. Entonces, un paso natural es considerar binomios que se componen de una suma de dos monomios de permutación. En este investigación se consideran dichos binomios.

2. Preliminares

Definición 2.1. Una **permutation** de un conjunto A es un reordenamiento de sus elementos. Esto se ve como una biyección $f : A \to A$.

Definición 2.2. Sea A un conjunto y $f(x)$ un polinomio. Entonces, se dice que $f(x)$ es un **polinomio de permutación** si $f : A \to A$ permuta los elementos de A, es decir, f es una biyección.

Definición 2.3. Un **cuerpo** $\mathbb{F}_q$ es una estructura algebraica que consiste de un conjunto finito A, de cardinalidad q, donde $q = p^r$ con p primo, con las operaciones + y *, que satisface los siguientes axiomas:

- A es **cerrado** bajo ambas operaciones.
- Ambas operaciones son **asociativas** en A.
- Ambas operaciones son **conmutativas** en A.
- Ambas operaciones tienen un **elemento identidad** en A.
- Todo elemento de A tiene una **inversa aditiva** y todo elemento de A distinto de 0 tiene una **inversa multiplicativa**.
- La operación * **distribuye** a la operación +.

Definición 2.4. Sea a elemento de $\mathbb{F}_q$. Entonces, a es una enésima **raíz unitaria** si satisface la ecuación $a^n = 1$.

Definición 2.5. Sea p primo. Un entero a es un residuo enésimo módulo p si existe x tal que $x^n \equiv a \ mod \ p$.

Teorema 2.1. (Teorema pequeño de Fermat) Sea a elemento $\mathbb{F}_q$, entonces $a^{q-1} = 1$.

Proposición 2.1 Sea p primo, K el conjunto de elementos de residuos $\frac{p-1}{n} \ mod \ p$ y H el conjunto de las enésimas raíces unitarias en $\mathbb{F}_q$. Entonces, $K = H$.

Demostración. Sea a elemento de K. Entonces, $a = x^{\frac{p-1}{n}}$ para alguna x en $\mathbb{F}_q$. Dado que $a^n = (x^{\frac{p-1}{n}})^n = x^{p-1} = 1$, a está en el conjunto H. Por tanto, K es subconjunto de H.

Note que $|K| = ny|H| = \frac{p-1}{\frac{p-1}{n}} = n$. Por lo tanto, como $|K| = |H|$ y K es subconjunto de H, entonces $K = H$.

Teorema 2.2. Sea $m > 0$. Entonces, x^m permuta $\mathbb{F}_q$ si y solo si $mcd(m, q-1) = 1$.

3. Trabajo Realizado

3.1. Resultados Computacionales

En este trabajo, se considera la pregunta sobre cuándo $x^m + Ax^n$ permuta, donde ambos x^m y Ax^n son monomios de permutación. Se comenzó verificando computacionalmente las sumas de todas las parejas de monomios de permutación, y cuándo estas permutan.

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
5	No hay permutaciones	$\frac{p-1}{2}$ primo
7	No hay permutaciones	$\frac{p-1}{2}$ primo
11	No hay permutaciones	$\frac{p-1}{2}$ primo
13	$x^n(x^{\frac{p-1}{2}} + A)$	$\frac{p-1}{4}$ primo
17	$x^n(x^{\frac{p-1}{2}} + A)$	-
19	$x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
23	No hay permutaciones	$\frac{p-1}{2}$ primo

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
29	$x^n(x^{\frac{p-1}{2}} + A)$	$\frac{p-1}{4}$ primo
31	$x^n(x^{\frac{p-1}{3}} + A)$	-
37	$x^n(x^{\frac{p-1}{2}} + A)$ $x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
41	$x^n(x^{\frac{p-1}{2}}) + A)$	-
43	$x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
47	No hay permutaciones	$\frac{p-1}{2}$ primo

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
53	$x^n(x^{\frac{p-1}{2}} + A)$	$\frac{p-1}{4}$ primo
59	No hay permutaciones	$\frac{p-1}{2}$ primo
61	$x^n(x^{\frac{p-1}{2}} + A)$ $x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$ $x^n(x^{\frac{p-1}{5}} + A)$ $x^n(x^{2(\frac{p-1}{5})} + A)$ $x^n(x^{3(\frac{p-1}{5})} + A)$	-
67	$x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
71	No hay permutaciones	-

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
73	$x^n(x^{\frac{p-1}{4}}+A)$ $x^n(x^{2(\frac{p-1}{4})}+A)$ $x^n(x^{3(\frac{p-1}{4})}+A)$ $x^n(x^{\frac{p-1}{3}}+A)$ $x^n(x^{2(\frac{p-1}{3})}+A)$	-
79	$x^n(x^{\frac{p-1}{3}}+A)$ $x^n(x^{2(\frac{p-1}{3})}+A)$	-
83	No hay permutaciones	$\frac{p-1}{2}$ prime
89	$x^n(x^{\frac{p-1}{4}}+A)$ $x^n(x^{2(\frac{p-1}{4})}+A)$ $x^n(x^{3(\frac{p-1}{4})}+A)$	-
97	$x^n(x^{\frac{p-1}{4}}+A)$ $x^n(x^{2(\frac{p-1}{4})}+A)$ $x^n(x^{3(\frac{p-1}{4})}+A)$ $x^n(x^{\frac{p-1}{3}}+A)$ $x^n(x^{2(\frac{p-1}{3})}+A)$	-

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
101	$x^n(x^{\frac{p-1}{2}} + A)$	-
103	$x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
107	No hay permutaciones	$\frac{p-1}{2}$ prime
109	$x^n(x^{\frac{p-1}{2}} + A)$ $x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
113	$x^n(x^{\frac{p-1}{4}} + A)$ $x^n(x^{2(\frac{p-1}{4})} + A)$ $x^n(x^{3(\frac{p-1}{4})} + A)$	-

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
127	$x^n(x^{\frac{p-1}{3}}+A)$ $x^n(x^{2(\frac{p-1}{3})}+A)$ $x^n(x^{\frac{p-1}{7}}+A)$ $x^n(x^{2(\frac{p-1}{7})}+A)$ $x^n(x^{3(\frac{p-1}{7})}+A)$ $x^n(x^{4(\frac{p-1}{7})}+A)$ $x^n(x^{5(\frac{p-1}{7})}+A)$ $x^n(x^{6(\frac{p-1}{7})}+A)$	-
131	$x^n(x^{\frac{p-1}{5}}+A)$ $x^n(x^{2(\frac{p-1}{5})}+A)$ $x^n(x^{3(\frac{p-1}{5})}+A)$ $x^n(x^{4(\frac{p-1}{5})}+A)$	-
137	$x^n(x^{\frac{p-1}{4}}+A)$ $x^n(x^{2(\frac{p-1}{4})}+A)$ $x^n(x^{3(\frac{p-1}{4})}+A)$	-
139	$x^n(x^{\frac{p-1}{3}}+A)$ $x^n(x^{2(\frac{p-1}{3})}+A)$	-

Primo (p)	Permutaciones en $\mathbb{F}_p$	Notas
149	$x^n(x^{\frac{p-1}{2}} + A)$	-
151	$x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-
157	$x^n(x^{\frac{p-1}{2}} + A)$ $x^n(x^{\frac{p-1}{3}} + A)$ $x^n(x^{2(\frac{p-1}{3})} + A)$	-

3.2. Forma de los Binomios

3.2.1. $\frac{p-1}{2}$ primo y $\frac{p-1}{4}$ primo

Partiendo de los resultados computacionales, lo primero que se consideró fue en qué cuerpos no existen binomios que sean sumas de monomios de permutación que permuten los elementos del cuerpo.

Lema 3.2.1. Si $p > 5$ es primo y $f(x) = x^m + Ax^n$ permuta $\mathbb{F}_p$, donde $m > n > 0$ y A es elemento de $\mathbb{F}_p^*$, entonces $mcd(m - n,\ p - 1)$ no es 2 o 4.

Lema 3.2.2. Sea k un número entero positivo. Si p es primo, entonces $mcd(k,\ 2p) \in \{1, 2, p, 2p\}$.

Demostración. Considere $2p$, donde p es primo. Los divisores de 2 son $\{1, 2\}$ y los divisores de p son $\{1, p\}$. Por lo tanto, los divisores de $2p$ son $\{1, 2, p, 2p\}$. Entonces, por definición, $mcd(k,\ 2p) \in \{1, 2, p, 2p\}$.

Proposición 3.2.1. Si $\frac{p-1}{2}$ es primo, entonces $f(x) = x^m + Ax^n$ no permuta $\mathbb{F}_p$, donde $mcd(m,\ p-1) = mcd(n,\ p-1) = 1$ y A es elemento de $\mathbb{F}_p^*$.

Demostración. Note que dado que $mcd(m,\, p-1) = mcd(n,\, p-1) = 1$, $m-n$ es par y $m-n < p-1$. Por lo tanto, $mcd(m-n,\, p-1) \neq \frac{p-1}{2}$, ya que $\frac{p-1}{2}$ es primo. Correspondientemente, $mcd(m-n,\, p-1) \neq p-1$, ya que $m-n < p-1$. Entonces, por el **Lema 3.2.2.**, las únicas posibilidades restantes para $mcd(m-n,\, p-1)$ son $\{1, 2\}$. Dado que $2 \mid m-n$, $2 \mid p-1$ y $2 < 1$, tenemos que $gcd(m-n, p-1) = 2$. Por el **Lema 3.2.1.1**, $x^m + Ax^n$ no permuta $\mathbb{F}_p$.

Corolario 3.2.1. Si $\frac{p-1}{4}$ es primo, entonces $f(x) = x^m + Ax^n$ es un polinomio de permutación solo si $m - n = \frac{p-1}{2}$, donde $mcd(m,\, p-1) = mcd(n,\, p-1) = 1$ y A es elemento de $\mathbb{F}_p^*$.

En los resultados computacionales se observó que todas las permutaciones dadas por binomios que son sumas de monomios de permutación pertenecen a la familia de polinomios $x^r(f(x^{\frac{p-1}{d}}))$. Específicamente, si $f(x) = x^m + Ax^n$ permuta $\mathbb{F}_p$, donde $mcd(m,\, p-1) = mcd(n,\, p-1)$, entonces $m - n = \frac{p-1}{d}$ o un múltiplo $k(\frac{p-1}{d})$ de $\frac{p-1}{d}$. Por tanto, se hace la siguiente conjetura.

Conjetura 3.2.1. Sea p primo, n, d, k enteros positivos, $d < k$ y $mcd(n,\, p-1)$ $= mcd(d,\, k) = 1$. Si existe A en $\mathbb{F}_p^*$ tal que xn(xk(p-1)/d + A) permute $\mathbb{F}_p$, entonces existe una B en $\mathbb{F}_p^*$ tal que $x^n(x^{h(\frac{p-1}{d})} + B)$ permute $\mathbb{F}_p$ para toda h donde $1 \leq h < k$.

3.3. Condición necesaria para que $x^n(x^{\frac{p-1}{d}} + A)$ permute $\mathbb{F}_p$

Al observar computacionalmente que las sumas de monomios de permutación de la forma $x^n(x^{\frac{p-1}{d}} + A)$ son los que producen permutaciones, es de interés caracterizar las A para las que $x^n(x^{\frac{p-1}{d}} + A)$ permuta.

Teorema 3.3.1. Sea $mcd(n,\, q-1) = 1$. Entonces $f(x) = x^n(x^{\frac{p-1}{2}} + A)$ es un polinomio de permutación en $\mathbb{F}_p$ si y solo si $A^2 - 1$ es un residuo cuadrático.

Partiendo de este teorema, y considerando $f(x) = x^n(x^{\frac{p-1}{d}} + A)$ para $d = 3$, se hizo un programa en SageMath en el que se verificó si una condición necesaria para que $f(x)$ permute $\mathbb{F}_p$ es que A^3+1 sea un residuo cúbico. Sucesivamente, se hicieron programas en SageMath en los que se verificó hasta $d = 7$, verificando la condición A^d+1 sea un residuo edésimo para d impar y A^d-1 sea un residuo edésimo para d par. Al tener estos casos ciertos, se obtuvo una base para una condición más general sobre d.

Conjetura 3.2.2. Sea $mcd(m,\, p-1) = 1$, A elemento de $\mathbb{F}_p^*$. Si $x^n(x^{\frac{p-1}{d}} + A)$ permuta $\mathbb{F}_p$, entonces $A^d + (-1)^{d+1}$ es un residuo edésimo.

4. Trabajo Futuro

- Dado que el conjunto de residuos $n \mod p$ es equivalente al conjunto de las $\frac{p-1}{d}$-ésimas raíces unitarias y gran cantidad de la literatura sobre los polinomios $x^r(f(x^{\frac{p-1}{d}}))$ se encuentra en términos de raíces unitarias, revisar la literatura para explorar las relaciones entre los criterios desarrollados y nuestras conjeturas.
- Probar **Conjetura 3.2.1** y **Conjetura 3.2.2**.

5. Presentaciones

- Presentación oral en el Junior Technical Meeting (JTM)/Puerto Rico Interdisciplinary Scientific Meeting (PRISM). (4 de mayo de 2019)

Referencias

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

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

[3] Lillian González, *Involuciones de Cuerpos Finitos Obtenidas por Binomios*, Technical Report 1, 2018.

[4] D. Burton *Elementary Number Theory*, Allyn and Bacon, Inc., 1980.

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