

Informe técnico sobre una clase de polinomios de permutación

Christian A. Rodríguez

Alex D. Santos

Universidad de Puerto Rico

Recinto de Río Piedras

Departamento de Ciencia de Cómputos

Resumen

El abstract lo dejamos para el final

1. Preliminares

Aquí van todos los preliminares sobre polinomios de permutación y un poco sobre la motivación de Francis a escoger el polinomio que estamos estudiando.

2. Nuestra clase de polinomios

Sea $p \equiv 1 \pmod{3}$. Nosotros consideramos el polinomio $F(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ definido sobre \mathbb{F}_p . Estudiamos maneras de hallar pares de $(a, b) \in \mathbb{F}_p$ tales que $F(x)$ sea un polinomio de permutación. Sabemos que todos los valores en \mathbb{F}_p pueden ser expresados como una potencia de la raíz primitiva α . La manera en que estudiamos esta clase de polinomios es considerando $x = \alpha^n$ para algún $n \in \mathbb{F}_p$. Esto es, consideramos $F(\alpha^n) = (\alpha^n)^{\frac{p+1}{2}} + a(\alpha^n)^{\frac{p+5}{6}} + b\alpha^n$. También note que podemos factorizar x , cambiando nuestro polinomio a $F(x) = x(x^{\frac{p-1}{2}} + ax^{\frac{p-1}{6}} + b)$. Más aún utilizamos el algoritmo de división para particionar \mathbb{F}_p en 6 clases. Es decir, consideramos $n = 6k + r$ donde $0 \leq r \leq 5$ y $0 \leq k \leq \frac{p-1}{6}$. Ahora $F(x)$ es particionado en 6 clases:

- $F(\alpha^{6k}) = \alpha^{6k}(1 + a + b)$
- $F(\alpha^{6k+1}) = \alpha^{6k}(-\alpha + a\alpha^{\frac{p+5}{6}} + b\alpha)$
- $F(\alpha^{6k+2}) = \alpha^{6k}(\alpha^2 + a\alpha^{\frac{p+5}{3}} + b\alpha^2)$
- $F(\alpha^{6k+3}) = \alpha^{6k}(-\alpha^3 - a\alpha^3 + b\alpha^3)$
- $F(\alpha^{6k+4}) = \alpha^{6k}(\alpha^4 + a\alpha^{2\frac{p+5}{3}} + b\alpha^4)$
- $F(\alpha^{6k+5}) = \alpha^{6k}(-\alpha^5 + a\alpha^{5\frac{p+5}{6}} + b\alpha^5)$

Procedemos a estudiar la cantidad de pares (a, b) que nos producen polinomios de permutación, y maneras de hallar estos pares.

3. Pares de a y b

Sabemos que si $F(x)$ es un polinomio de permutación, entonces $F(x) = 0$ si y solo si $x = 0$. También sabemos que $\alpha^n \neq 0$ para toda $n \in \mathbb{F}_p$. Ahora con $F(x) = 0$ podemos obtener algunas condiciones en los pares (a, b) tal que $F(x)$ no es de permutación.

Lemma 1. *Sea $F(x) = x(x^{\frac{p-1}{2}} + ax^{\frac{p-1}{6}} + b)$. Utilizando las 6 clases que describimos arriba, se obtiene que los siguientes pares de (a, b) no producen una permutación:*

- $F(\alpha^{6k}) = 0 \rightarrow [a, -1 - a]$
- $F(\alpha^{6k+1}) = 0 \rightarrow [a, 1 - a\alpha^{\frac{p-1}{6}}]$
- $F(\alpha^{6k+2}) = 0 \rightarrow [a, -1 - a\alpha^{\frac{p-1}{3}}]$
- $F(\alpha^{6k+3}) = 0 \rightarrow [a, 1 + a]$
- $F(\alpha^{6k+4}) = 0 \rightarrow [a, -1 - a\alpha^{2*\frac{p-1}{3}}]$
- $F(\alpha^{6k+5}) = 0 \rightarrow [a, 1 - a\alpha^{5*\frac{p-1}{6}}]$

4. Cantidad de permutaciones

Ejemplos que hemos calculado nos llevan a la siguiente conjetura:

Conjetura 1. *Considere el polinomio $F(x)$. Si (a, b) produce una permutación, entonces $(a, -b)$ también produce una permutación.*

En el caso de $p = 31$ hemos podido demostrar esta conjetura. Hallamos una correspondencia entre las clases de arriba al evaluar el polinomio en (a, b) y al evaluarlo en $(a, -b)$, de esta manera demostrando que cuando uno de los pares produce un polinomio de permutación el otro también.

Demostración. Sea $P_{31}(x, a, b) = x(x^{\frac{p-1}{2}} + ax^{\frac{p-1}{6}} + b)$ definido sobre \mathbb{F}_{31} . Demostraremos que $P_{31}(\alpha^{6k+i}, a, b) = P_{31}(\alpha^{6l+j}, a, -b)$ donde

$$l = \begin{cases} k + 2 \text{ mód } 5, & 0 \leq i \leq 2 \\ k + 3 \text{ mód } 5, & 3 \leq i \leq 5 \end{cases}$$

,

$$j = \begin{cases} i + 3, & 0 \leq i \leq 2 \\ i - 3, & 3 \leq i \leq 5 \end{cases}$$

Primero note que

$$\begin{aligned} P_{31}(\alpha^{6k+i}, a, b) &= \alpha^{6k+i}((\alpha^{6k+i})^{\frac{p-1}{2}} + a(\alpha^{6k+i})^{\frac{p-1}{6}} + b) \\ &= \alpha^{6k+i}((-1)^i + a\alpha^{i\frac{p-1}{6}} + b) \end{aligned}$$

También note que

$$\begin{aligned} 6(k+2) + i + 3 &= 6k + 12 + i + 3 = 6k + i + 15 \\ 6(k+3) + i - 3 &= 6k + 18 + i - 3 = 6k + i + 15 \end{aligned}$$

Finalmente:

$$\begin{aligned} P_{31}(\alpha^{6l+j}, a, -b) &= -\alpha^{6k+i}((-\alpha^{6k+i})^{\frac{p-1}{2}} + a(-\alpha^{6k+i})^{\frac{p-1}{6}} - b) \\ &= -\alpha^{6k+i}((-1)^{\frac{p-1}{2}}(\alpha^{6k+i})^{\frac{p-1}{2}} + a(-1)^{\frac{p-1}{6}}(\alpha^{6k+i})^{\frac{p-1}{6}} - b) \\ &= -\alpha^{6k+i}(-(-1)^i - a\alpha^{i\frac{p-1}{6}} - b) \\ &= \alpha^{6k+i}((-1)^i + a\alpha^{i\frac{p-1}{6}} + b) \end{aligned}$$

□

Nuestra demostración utiliza el hecho de que $\frac{p-1}{2} = \frac{30}{2} = 15$ es impar. En la generalización debe existir otra variable que haga que funcione cuando $\frac{p-1}{2}$ sea par.

Referencias

Necesitamos añadir referencias.