Permutation Polynomials

Christian A. Rodríguez; Alex D. Santos; Ivelisse Rubio; Francis Castro;
Department of Computer Science

Abstract

Dado un trinomio de la forma $f_{a,b}(X) = X^r(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$ sobre un cuerpo finito $\mathbb{F}_q$ con tamaño de value set s, construímos $d = lcm(d_1, d_2)$ otros trinomios en $\mathbb{F}_q$ con el mismo tamaño de value set. En particular, dado un polinomio de permutación de la forma $f_{a,b}$, construímos $d = lcm(d_1, d_2)$ otros polinomios de permutación en $\mathbb{F}_q$. También construímos secuencias $P_{q^{m_1}}, P_{q^{m_2}}, \cdots$, donde $P_{q^{m_i}}$ es un polinomio de permutación en $\mathbb{F}_{q^{m_i}}$.

Preliminares

Definición. *Una* ***permutación*** *de un conjunto A es un ordenamiento de los elementos de A. Una funcion $f : A \to A$ nos da una permutación de A si y solo si f es uno a uno y sobre.*

Definición. *Un* ***cuerpo finito*** *$\mathbb{F}_q$, $q = p^r$, p primo, es un conjunto con $q = p^r$ elementos.*

Definición. *Una* ***raiz primitiva*** *$\alpha \in \mathbb{F}_q$ es un generador del grupo multiplicativo $\mathbb{F}_q^*$.*

Ejemplo. *Considere el cuerpo finito $\mathbb{F}_7$. Tenemos que: $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$, entonces 3 es una raiz primitiva de $\mathbb{F}_7$.*

Definición. *Sea $f(x)$ un polinomios definido sobre $\mathbb{F}_q$. El* ***value set*** *de f esta definido por $V_f = \{f(a) \mid a \in \mathbb{F}_q\}$.*

Note que un polinomios $f(x)$ definido por $\mathbb{F}_q$ es un polinomio de permutación si y solo si $V_f = \mathbb{F}_q$.

Problema

Estudiar el value set de polinomios de la forma

$$F_{a,b}(X) = X(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$$

sobre cuerpos finitos $\mathbb{F}_q$ y determinar condiciones en a, b tal que el polinomio es un polinomio de permutación.

Resultados - Value Sets

Definimos una relación para construir clases de equivalencia de polinomios con value sets de la misma cardinalidad.

Definición 1. *Sean $a = \alpha^i, b = \alpha^j$, donde α es una raiz primitiva en $\mathbb{F}_q$, y $\sim$ una relación en $\mathbb{F}_q^* \times \mathbb{F}_q^*$ definida por: $(a, b) \sim (a', b')$ $\iff a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}$, donde $h \in \mathbb{Z}$.*

Ejemplo. *Sean $q = 13, d_1 = 2, d_2 = 3$, entonces tenemos $\alpha = 2$ y $a = 2^2 = 4, b = 2^3 = 8$. Ahora $(a, b) \sim (a', b')$ si y solo si $a' = \alpha^{2+2h}, b' = \alpha^{3+6h}$. Por ejemplo $(2^2, 2^3) \sim (2^{2+2}, 2^{3+6})$.*

Lema 1. *La relación $\sim$ en Def 1 en una relación de equivalencia en $\mathbb{F}_q^* \times \mathbb{F}_q^*$.*

La relación de equivalencia definida anteriormente induce una relación de equivalencia en el conjunto de polinomios de la forma $F_{a,b}(X) = X(X^{\frac{q-1}{d_1}} + aX^{\frac{q-1}{d_2}} + b)$ con clases de equivalencia $[F_{a,b}] = [F_{\alpha^i,\alpha^j}] = \left\{ F_{a',b'} | a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})} \right\}$. Esto provee una construcción para polinomios con value sets de la misma cardinalidad.

Teorema 1. *Suponer que $F_{a,b} \sim F_{a',b'}$ donde $\sim$ es la relación de equivalencia en el Lema 1. Entonces $|V(F_{a,b})| = |V(F_{a',b'})|$.*

Número de Polinomios de Permutación