



# Generating Families of Permutation Trinomials

Christian A. Rodríguez; Alex D. Santos  
Department of Computer Science,  
University of Puerto Rico, Rio Piedras Campus

## RESUMEN

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 un conjunto de valores de tamaño  $s$ , construimos otros  $d$  trinomios en  $\mathbb{F}_q$  con el mismo tamaño de conjunto de valores, donde  $d = mcm(d_1, d_2)$ . En particular, dado un polinomio de permutación de la forma  $f_{a,b}$ , construimos  $d$  otros polinomios de permutación en  $\mathbb{F}_q$ . También generamos secuencias  $P_q^{m_1}, P_q^{m_2}, \dots$ , 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 función  $f : A \rightarrow A$  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 *raíz 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 raíz primitiva de  $\mathbb{F}_7$ .

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

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

## APLICACIONES

- El operador de encriptación de algunos sistemas de encriptación es una permutación de un cuerpo finito  $\mathbb{F}_q$  y necesita ser computado eficientemente. Si expresamos ese operador en términos de un polinomio, computarlo es simple y eficiente.
- Polinomios con conjuntos de valores mínimos están relacionados a curvas con un número grande de puntos racionales.

## RESULTADOS - CONJUNTOS DE VALORES

Definimos una relación para construir clases de equivalencia de polinomios con conjuntos de valores de la misma cardinalidad.

**Definición 1.** Sean  $a = \alpha^i, b = \alpha^j$ , donde  $\alpha$  es una raíz primitiva en  $\mathbb{F}_q$ , y  $\sim$  una relación en  $\mathbb{F}_q^* \times \mathbb{F}_q^*$  definida por:  $(a, b) \sim (a', b')$

$$\iff a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})}, \text{ donde } h \in \mathbb{Z}.$$

**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 es una relación de equivalencia en  $\mathbb{F}_q^* \times \mathbb{F}_q^*$ .

El Lema 1 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  $[F_{a,b}] = [F_{\alpha^i, \alpha^j}] = \left\{ F_{a',b'} \mid a' = \alpha^{i+h(\frac{q-1}{d_1} - \frac{q-1}{d_2})}, b' = \alpha^{j+h(\frac{q-1}{d_1})} \right\}$ .

Esto provee una construcción para polinomios con conjuntos de valores de la misma cardinalidad.

**Teorema 2.** Suponer que  $F_{a,b} \sim F_{a',b'}$  donde  $\sim$  es la relación de equivalencia en el Lema 1. Entonces  $|V(F_{a,b})| = |V(F_{a',b'})|$ .

## PROBLEMA

Estudiar el conjunto de valores 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 - PERMUTACIÓN

**Proposición 1.**  $|[F_{a,b}]| = mcm(d_1, d_2)$ .

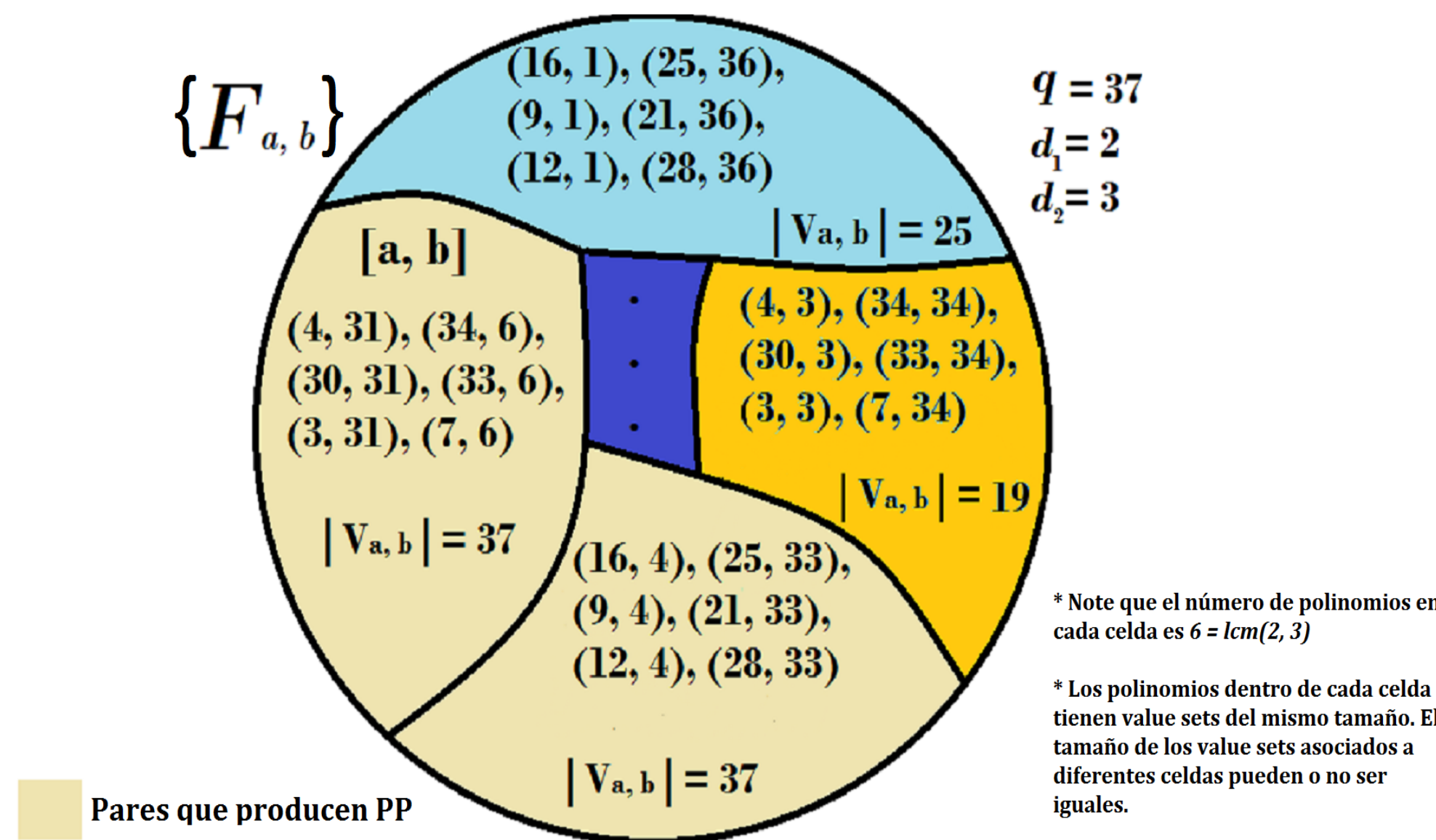
Dado un polinomio podemos construir otros  $mcm(d_1, d_2)$  polinomios con conjunto de valores de la misma cardinalidad:

$$(\alpha^2, \alpha^{26}), (\alpha^8, \alpha^8), (\alpha^{14}, \alpha^{26}), (\alpha^{20}, \alpha^8), (\alpha^{26}, \alpha^{26}), (\alpha^{32}, \alpha^8)$$

**Teorema 1.** El número de polinomios de la forma  $F_{a,b}(X)$  con  $|V_{a,b}| = n$  es un múltiplo de  $mcm(d_1, d_2)$ .

Un resultado directo del Teorema 1 es el caso particular cuando  $|V_{a,b}| = q$ , esto implica que tenemos polinomios de permutación. La construcción establecida anteriormente nos provee una manera de construir familias de polinomios de permutación.

**Corolario 1.** El número de polinomios de permutación de la forma  $F_{a,b}(X)$  es un múltiplo de  $mcm(d_1, d_2)$ .



## TRABAJO FUTURO

- Encontrar condiciones suficientes y necesarias tal que  $V_{a,b} = \mathbb{F}_q$  y  $V_{a,b}$  sea de cardinalidad mínima.
- Generalizar los resultados a polinomios con más términos y con exponentes no divisores de  $q - 1$ :  $f_{a,b}(X) = X^r(X^{d_1} + aX^{d_2} + b)$ .

## REFERENCIAS

- [1] Panario, D., Mullen, G., *Handbook of Finite Fields*. CRC Press (2013).
- [2] Wan, D., Lidl, R. *Permutation Polynomials of the Form  $x^r f(x^{\frac{q-1}{d}})$  and Their Group Structure*. Mh. Math. 112, 149-163 (1991).
- [3] Borges, H., Conceicao R. *On the characterization of minimal conjunto de valores polynomial*. Journal of Number Theory 133 (2013) 2021-2035.