On a Class of Permutation Polynomials over Finite Fields

November 20, 2013

Abstract

1 Results

Definition 1.1. Sea $a = \alpha^i, b = \alpha^j$ y $\sim$ la relacion definida por $(a, b) \sim (a', b')$ $<=> a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b' = \alpha^{j+h(\frac{p-1}{d_1})}$

Proposition 1.2. $\sim$ definida arriba es una relación de equivalencia.

Proof. Pendiente

□

Proposition 1.3. Sea $[a, b]$ la clase de equivalencia de (a, b). Si $(a', b') \in [a, b]$, entonces $|V_{a',b'}| = |V_{a,b}|$

Proof. Sea α la raiz primitiva del cuerpo finito.

$$F_{a',b'}(\alpha^{k+1}) = \alpha^{k+1}((\alpha^{k+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k+1}((\alpha^k)^{\frac{p-1}{d_1}} \cdot \alpha^{\frac{p-1}{d_1}} + \alpha^i \cdot \frac{\alpha^{\frac{p-1}{d_1}}}{\alpha^{\frac{p-1}{d_2}}}(\alpha^k)^{\frac{p-1}{d_2}} \cdot \alpha^{\frac{p-1}{d_2}} + \alpha^j \cdot \alpha^{\frac{p-1}{d_1}})$$

$$= \alpha^{\frac{p-1}{d_1}+1} \cdot \alpha^k((\alpha^k)^{\frac{p-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^j)$$

$$= C \cdot F_{a,b}(\alpha^k), \text{donde } C = \alpha^{\frac{p-1}{d_1}+1}$$

En general para cada termino de $F_{a,b}(\alpha^k)$ va a haber un termino correspondiente de $F_{a',b'}(\alpha^{k+1})$ donde $a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$ y $b' = \alpha^{j+h(\frac{p-1}{d_1})}$. Por otra parte, debe ser el caso de que $\left|V_{F_{a,b}}\right| = \left|V_{F_{a',b'}}\right|$.

□

Proposition 1.4. Si $d_2 = d_1 \cdot h$, entonces $|[a, b]| = d_2$

Proof. Note that we can repeat this process using $a'' = a' \cdot \alpha^{(d+2)(\frac{q-1}{2d})}$, $b'' = b' \cdot \alpha^{(\frac{q-1}{2})}$. We argue that this process can be repeated at most $d-1$ times when d is even, and $2d-1$ times when d is odd. $\square$

Proposition 1.5. Suponga que $d_2 = d_1 \cdot h + r$, $1 \leq r \geq d_1$. Entonces, $|[a, b]| = \frac{d_1 \cdot d_2}{?}$

Proposition 1.6. El número de polinomios $F_{a',b'}(x)$ con $|V_{a,b}|$ es un múltiplo de $|[a, b]|$