

# On a Class of Permutation Polynomials over Finite Fields

November 18, 2013

**Abstract**

## 1 Results

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

**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  $\alpha$  la raiz primitiva del cuerpo finito.

$$\begin{aligned} F_{a', b'}(\alpha^{k+1}) &= \alpha^{k+1}((\alpha^{k+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}}) \\ &= \alpha^{k+1}((\alpha^k)^{\frac{p-1}{d_1}} \cdot \alpha^{\frac{p-1}{d_1}} + \alpha^i \cdot \frac{\alpha^{\frac{p-1}{d_1}}}{\alpha^{\frac{p-1}{d_2}}}(\alpha^k)^{\frac{p-1}{d_2}} \cdot \alpha^{\frac{p-1}{d_2}} + \alpha^j \cdot \alpha^{\frac{p-1}{d_1}}) \\ &= \alpha^{\frac{p-1}{d_1}+1} \cdot \alpha^k((\alpha^k)^{\frac{p-1}{d_1}} + \alpha^i(\alpha^k)^{\frac{p-1}{d_2}} + \alpha^j) \\ &= C \cdot F_{a, b}(\alpha^k), \text{ donde } C = \alpha^{\frac{p-1}{d_1}+1} \end{aligned}$$

□

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

*Proof.* Pendiente, hay que hacerla pa mañana!!

□

**Proposition 1.5.** Suponga que  $d_2 = d_1 \cdot h + r$ ,  $1 \leq r \leq d_1$ . 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  $||[a, b]||$