

# On a Class of Permutation Polynomials over Finite Fields

November 21, 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.* 1. Sea  $a = \alpha^i, b = \alpha^j$  y escoja  $h = 0$ . Entonces  $a' = \alpha^{i+0(\frac{p-1}{d_1}-\frac{p-1}{d_2})} = \alpha^i = a$  y  $b' = \alpha^{j+0(\frac{p-1}{d_1})} = \alpha^j = b$ . Por lo tanto  $(a, b) \sim (a, b)$  y la relacion es reflexiva.

2. Sea  $a = \alpha^i, b = \alpha^j, a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$  y  $b' = \alpha^{j+h(\frac{p-1}{d_1})}$  entonces  $(a, b) \sim (a', b')$ . Queremos encontrar  $l$  tal que  $a = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})+l(\frac{p-1}{d_1}-\frac{p-1}{d_2})}$  y  $b = \alpha^{j+h(\frac{p-1}{d_1})+l(\frac{p-1}{d_1})}$ . Escoja  $l = d_1 d_2 - h$ , entonces obtenemos:  $\alpha^{i+d_1 d_2(\frac{p-1}{d_1}-\frac{p-1}{d_2})} = \alpha^i = a$  y  $\alpha^{j+d_1 d_2(\frac{p-1}{d_1})} = \alpha^j = b$ . Por lo tanto  $(a', b') \sim (a, b)$  y la relacion es simetrica.

3. Suponga que  $a = \alpha^i, b = \alpha^j, a' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b' = \alpha^{j+h(\frac{p-1}{d_1})}, a'' = \alpha^{i+h(\frac{p-1}{d_1}-\frac{p-1}{d_2})+l(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b'' = \alpha^{j+h(\frac{p-1}{d_1})+l(\frac{p-1}{d_1})}$ . Por lo tanto  $(a, b) \sim (a', b')$  y  $(a', b') \sim (a'', b'')$ . Ahora note que  $a'' = \alpha^{i+(h+l)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b'' = \alpha^{j+(h+l)(\frac{p-1}{d_1})}$ , por lo tanto  $(a, b) \sim (a'', b'')$  y la relacion es transitiva.

Como la relacion es reflexiva, simetrica y transitiva, concluimos que es una relacion de equivalencia. □

**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.

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

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

□

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

*Proof.* Suponga que  $d_2 = d_1 h$ ,  $a = \alpha^i$ ,  $b = \alpha^j$ . Note que podemos obtener los elementos de  $[a, b]$  aplicando la transformacion  $f : (a, b) \rightarrow (a \cdot \alpha^{(\frac{p-1}{d_1} - \frac{p-1}{d_2})}, b \cdot \alpha^{(\frac{p-1}{d_1})})$  multiples veces. Ahora note que:

$$f(a \cdot \alpha^{i+(d_2-1)(\frac{p-1}{d_1} - \frac{p-1}{d_2})}, b \cdot \alpha^{j+(d_2-1)(\frac{p-1}{d_1})}) \quad (1.1)$$

$$= (\alpha^{i+d_2(\frac{p-1}{d_1} - \frac{p-1}{d_2})}, \alpha^{j+d_2(\frac{p-1}{d_1})}) \quad (1.2)$$

$$= (\alpha^{i+d_1 h(\frac{p-1}{d_1}) - d_2(\frac{p-1}{d_2})}, \alpha^{j+d_1 h(\frac{p-1}{d_1})}) \quad (1.3)$$

$$= (\alpha^{i+h(p-1)-(p-1)}, \alpha^{j+h(p-1)}) \quad (1.4)$$

$$= (\alpha^i, \alpha^j) \quad (1.5)$$

Por lo tanto al aplicar la transformacion  $d_2$  veces, tendremos una cadena de elementos en  $[a, b]$ . Ahora suponga que existe  $c < d_2$  y  $\alpha^{i+c(\frac{p-1}{d_1} - \frac{p-1}{d_2})} = \alpha^i$  y  $\alpha^{j+c(\frac{p-1}{d_1})} = \alpha^j$ . Esto implica que  $\alpha^{c(\frac{p-1}{d_1} - \frac{p-1}{d_2})} = 1$ , luego  $\alpha^{c(\frac{p-1}{d_1}) - c(\frac{p-1}{d_2})} = 1$ , esto solo es posible si  $c \mid d_1$  y  $c \mid d_2$ , pero  $c < d_2$ . Por contradiccion,  $d_2$  es el elemento mas pequeno tal que esto ocurre. Por lo tanto la cantidad de elementos en la clase de equivalencia  $[a, b]$  es de tamano  $d_2$ .

□

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

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