On a Class of Permutation Polynomials over Finite Fields

December 17, 2013

Abstract

1 Results

Definition 1.1. Sean $d_1, d_2 \in \mathbb{F}_p$ tales que $d_1 \mid p$ y $d_2 \mid p$. Definimos el polinomio $F_{a,b}(x) = x(x^{\frac{p-1}{d_1}} + ax^{\frac{p-1}{d_2}} + b)$ con $a, b \in \mathbb{F}_q^{\times}$ y definimos $V_{a,b} = Im(F_{a,b}(x))$.

Definition 1.2. 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 1.3. $\sim$ 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 1.4. 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 $\left|V_{F_{a,b}}\right| = \left|V_{F_{a',b'}}\right|$.

Sea $f : V_{a',b'} \to \alpha^{\frac{p-1}{d_1}} V_{a,b}$ dada por $f(F_{a',b'}(\alpha^{k+1})) = \alpha^{\frac{p-1}{d_1}+1}F_{a,b}(\alpha^k)$. Suponga que $f(F_{a',b'}(\alpha^{k_1+1})) = f(F_{a',b'}(\alpha^{k_2+1}))$ donde $k_1, k_2 \in \mathbb{F}_q$.

Considere $f(F_{a',b'}(\alpha^{k_1+1}))$

$$= f(\alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1+1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{\frac{p-1}{d_1}+1}(\alpha^{k_1}((\alpha^{k_1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_1+1}(\alpha^{\frac{p-1}{d_1}}((\alpha^{k_1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}+\frac{p-1}{d_2}}(\alpha^{k_1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k_1+1}((\alpha^{k_1+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k_1+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= F_{a',b'}(\alpha^{k_1+1})$$

Luego considere $f(F_{a',b'}(\alpha^{k_2+1}))$

$$= f(\alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2+1})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{\frac{p-1}{d_1}+1}(\alpha^{k_2}((\alpha^{k_2})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_2+1}(\alpha^{\frac{p-1}{d_1}}((\alpha^{k_2})^{\frac{p-1}{d_1}} + \alpha^i(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^j))$$

$$= \alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}+\frac{p-1}{d_2}}(\alpha^{k_2})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= \alpha^{k_2+1}((\alpha^{k_2+1})^{\frac{p-1}{d_1}} + \alpha^{i+\frac{p-1}{d_1}-\frac{p-1}{d_2}}(\alpha^{k_2+1})^{\frac{p-1}{d_2}} + \alpha^{j+\frac{p-1}{d_1}})$$

$$= F_{a',b'}(\alpha^{k_2+1})$$

En conclusión $F_{a',b'}(\alpha^{k_1+1}) = F_{a',b'}(\alpha^{k_2+1})$ por lo tanto f es una función $1-1$

Considere un elemento en el campo de valores dado por $\alpha^{\frac{p-1}{d_1}} F_{a,b}(\alpha^k)$

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

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

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

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

$$= F_{a',b'}(\alpha^{k+1})$$

En conclusión para cada elemento en el campo de valores, $\alpha^{\frac{p-1}{d_1}} F_{a,b}(\alpha^k)$, existe un elemento en el dominio, $F_{a',b'}(\alpha^{k+1})$. Por lo tanto f es una función sobre y podemos concluir que $|V_{a',b'}| = |V_{a,b}|$.

□

Proposition 1.5. $|[a,b]| = lcm(d_1, d_2)$ donde $lcm(x,y)$ es el minimo común múltiplo de x y y.

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

$$\begin{aligned}
&f(a \cdot \alpha^{i+(lcm(d_1,d_2)-1)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, b \cdot \alpha^{j+(lcm(d_1,d_2)-1)(\frac{p-1}{d_1})})\\
&= (\alpha^{i+lcm(d_1,d_2)(\frac{p-1}{d_1}-\frac{p-1}{d_2})}, \alpha^{j+lcm(d_1,d_2)(\frac{p-1}{d_1})})\\
&= (\alpha^{i+lcm(d_1,d_2)(\frac{p-1}{d_1})-lcm(d_1,d_2)(\frac{p-1}{d_2})}, \alpha^{j+lcm(d_1,d_2)(\frac{p-1}{d_1})})\\
&= (\alpha^{i+\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_1})-\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_2})}, \alpha^{j+\frac{d_1d_2}{gcd(d_1,d_2)}(\frac{p-1}{d_1})})\\
&= (\alpha^{i+\frac{d_2}{gcd(d_1,d_2)}(p-1)-\frac{d_2}{gcd(d_1,d_2)}(p-1)}, \alpha^{j+\frac{d_2}{gcd(d_1,d_2)}(p-1)})\\
&= (\alpha^i, \alpha^j)
\end{aligned}$$

Por lo tanto al aplicar la transformacion $lcm(d_1, d_2)$ veces, tendremos una cadena de elementos en $[a,b]$. Ahora suponga que existe $c < lcm(d_1, d_2)$ tal que $\alpha^{i+c(\frac{p-1}{d_1}-\frac{p-1}{d_2})} = \alpha^i$ 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 es multiplo de d_1 y d_2 pero $c < lcm(d_1, d_2)$ y $lcm(d_1, d_2)$ 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 tamaño $lcm(d_1, d_2)$.

□

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