On a Class of Permutation Polynomials over Finite Fields

Francis Castro
José Ortiz
Christian A. Rodríguez
Ivelisse Rubio
Alex D. Santos
University of Puerto Rico, Río Piedras
Department of Computer Science

Alex y Yo demostramos la conjetura, aunque esta medio chapusiao por ahora. Lo importante es que tenemos la idea:

Theorem 1. *Sea p un primo y $d = 2 \cdot m$, m primo impar tal que $d \mid p-1$. Sea $F_{\alpha^i,\alpha^j}(x)$ polinomio de permutacin en $\mathbb{F}_p$. Tenemos que $(\alpha^{\frac{p-1}{2}-(m+2)} \cdot F_{\alpha^i,\alpha^j}(\alpha^l)) = F_{\alpha^{i+\frac{p-1}{m}},\alpha^{j+\frac{p-1}{2}}}(\alpha^k)$ donde $k, l \in \mathbb{F}_p^\times$ y $l = k+m+2$*

Tenemos el problema que l puede ser 0 y eso no es bueno.(Alex sabe porque)

Proof. Vamos a establecer una correspondencia entre los dos terminos. La correspondencia es la siguiente:

$F_{\alpha^{i+\frac{p-1}{m}},\alpha^{j+\frac{p-1}{2}}}(\alpha^k) = \alpha^k((\alpha^k)^{\frac{p-1}{2}} + (\alpha^{i+\frac{p-1}{m}}) \cdot (\alpha^k)^{\frac{p-1}{d}} + \alpha^{j+\frac{p-1}{2}})$

$= \alpha^k((\alpha^k)^{\frac{p-1}{2}} + (\alpha^{i+\frac{p-1}{m}}) \cdot (\alpha^k)^{\frac{p-1}{d}} - \alpha^j)$

$= -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{m}}) \cdot (\alpha^k)^{\frac{p-1}{d}} + \alpha^j)$

$= -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{m}} \cdot \alpha^{\frac{pk-k}{d}}) + \alpha^j)$

Note que si encontramos l tal que $(\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{m}} \cdot \alpha^{\frac{pk-k}{d}}) = (\alpha^l)^{\frac{p-1}{d}}$ estaremos un paso mas cerca. Simplificando obtenemos

$(\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{m}}) = \alpha^{\frac{pd-d+pkm-mk}{md}+\frac{p-1}{2}} = \alpha^{\frac{2pd-2d+2pkm-2mk+pmd-md}{2dm}} = \alpha^{\frac{(2d+2km+md)p-(2d+2km+md)}{2dm}}$

$= (\alpha^{\frac{2d+2km+md}{2m}})^{\frac{p-1}{d}}$
Por lo tanto tenemos que $l = \frac{2d+2km+md}{2m} = 2 + k + m$
Ahora $F_{\alpha^{i+\frac{p-1}{m}}, \alpha^{j+\frac{p-1}{2}}}(\alpha^k) = -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$
Luego, $k = l - m - 2$
$= -\alpha^{l-m-2}(-(-1)^{l-m-2} + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$
$= -\alpha^{-m-2} \cdot \alpha^l((-1)^l + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$
$= (-\alpha^{-m-2}) \cdot F_{\alpha^i,\alpha^j}(\alpha^l)$ □

Utilizando esta conjetura, demostramos el lemita sobre la cantidad de polinomios de permutacion de la forma $F_{a,b}(x)$:

Lemma 1. *Sea p un primo y $d = 2 \cdot m$ tal que m es impar. Sea n la cantidad de pares $[a, b]$ tal que $F_{a,b}(x)$ es un polinomio de permutacion en $\mathbb{F}_p$. Entonces tenemos que $d \mid n$.*

Proof. Si $n = 0$ es trivial, pues $d \mid 0$. Suponemos que $n \neq 0$. Sea $[a = \alpha^i, b = \alpha^j]$ un par tal que $F_{a,b}(x)$ es un polinomio de permutacion. Por el teorema 1 tenemos que $[\alpha^{i+\frac{p-1}{m}}, \alpha^{j+\frac{p-1}{2}}]$ tambien produce un polinomio de permutacion. De nuevo por el teorema 1 tenemos que $[\alpha^{i+2\cdot\frac{p-1}{m}}, \alpha^{j+2\cdot\frac{p-1}{2}}]$ nos produce un polinomio de permutacion. Nuestro argumento es que este proceso se puede repetir a lo sumo $d - 1$ veces. En la repeticion d obtenemos $[\alpha^{i+d\cdot\frac{p-1}{m}} = \alpha^i, \alpha^{j+d\cdot\frac{p-1}{2}} = \alpha^j]$. Por lo tanto por cada par $[a, b]$, obtenemos un conjunto de d pare tal que cada par nos produce un polinomio de permutacion: $\Big\{[\alpha^i, \alpha^j], [\alpha^{i+\frac{p-1}{m}}, \alpha^{j+\frac{p-1}{2}}], [\alpha^{i+2\cdot\frac{p-1}{m}}, \alpha^{j+2\cdot\frac{p-1}{2}}], \cdots, [\alpha^{i+(d-1)\cdot\frac{p-1}{m}}, \alpha^{j+(d-1)\cdot\frac{p-1}{2}}]\Big\}$. Esto implica que la cantidad de pares es $n = d \cdot q, q \in \mathbb{N}$. Por lo tanto $d \mid n$. □

Tambien demostramos la conjetura cuando m es par. Ahora si que somos los duros.

Theorem 2. *Sea p un primo y $d = 2 \cdot m$, m primo par tal que $d \mid p - 1$. Sea $F_{\alpha^i,\alpha^j}(x)$ polinomio de permutacin en $\mathbb{F}_p$. Tenemos que $(-\alpha^{-m-1} \cdot F_{\alpha^i,\alpha^j}(\alpha^l)) = F_{\alpha^{i+\frac{p-1}{d}}, \alpha^{j+\frac{p-1}{2}}}(\alpha^k)$ donde $k, l \in \mathbb{F}_p^\times$ y $l = k + m + 1$*

Proof. Vamos a establecer una correspondencia entre los dos terminos. La correspondencia es la siguiente:
$F_{\alpha^{i+\frac{p-1}{d}}, \alpha^{j+\frac{p-1}{2}}}(\alpha^k) = \alpha^k((\alpha^k)^{\frac{p-1}{2}} + (\alpha^{i+\frac{p-1}{d}}) \cdot (\alpha^k)^{\frac{p-1}{d}} + \alpha^{j+\frac{p-1}{2}})$
$= \alpha^k((\alpha^k)^{\frac{p-1}{2}} + (\alpha^{i+\frac{p-1}{d}}) \cdot (\alpha^k)^{\frac{p-1}{d}} - \alpha^j)$

$= -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{d}}) \cdot (\alpha^k)^{\frac{p-1}{d}} + \alpha^j)$
$= -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{d}} \cdot \alpha^{\frac{pk-k}{d}}) + \alpha^j)$

Note que si encontramos l tal que $(\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{d}} \cdot \alpha^{\frac{pk-k}{d}}) = (\alpha^l)^{\frac{p-1}{d}}$ estaremos un paso mas cerca. Simplificando obtenemos
$(\alpha^{\frac{p-1}{2}} \cdot \alpha^{\frac{p-1}{m}} \cdot \alpha^{\frac{pk-k}{d}}) = \alpha^{\frac{p+pk-k-1}{d}+\frac{p-1}{2}} = \alpha^{\frac{pd-d+2p+2kp-2k-2}{2d}} = \alpha^{\frac{(d+2+2k)p-(d+2+2k)}{2d}}$
$= (\alpha^{\frac{d+2+2k}{2}})^{\frac{p-1}{d}}$

Por lo tanto tenemos que $l = \frac{d+2+2k}{2} = k + m + 1$

Ahora $F_{\alpha^{i+\frac{p-1}{m}}, \alpha^{j+\frac{p-1}{2}}}(\alpha^k) = -\alpha^k(-(-1)^k + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$

Luego, $k = l - m - 1$
$= -\alpha^{l-m-1}(-(-1)^{l-m-1} + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$
$= -\alpha^{-m-1} \cdot \alpha^l((-1)^l + \alpha^i \cdot (\alpha^l)^{\frac{p-1}{d}} + \alpha^j)$
$= (-\alpha^{-m-1}) \cdot F_{\alpha^i,\alpha^j}(\alpha^l)$ □

Para este caso tambien tenemos el lemita:

Lemma 2. *Sea p un primo y $d = 2 \cdot m$ tal que m es par. Sea n la cantidad de pares $[a, b]$ tal que $F_{a,b}(x)$ es un polinomio de permutacion en $\mathbb{F}_p$. Entonces tenemos que $d \mid n$.*

Proof. Si $n = 0$ es trivial, pues $d \mid 0$. Suponemos que $n \neq 0$. Sea $[a = \alpha^i, b = \alpha^j]$ un par tal que $F_{a,b}(x)$ es un polinomio de permutacion. Por el teorema 1 tenemos que $[\alpha^{i+\frac{p-1}{d}}, \alpha^{j+\frac{p-1}{2}}]$ tambien produce un polinomio de permutacion. De nuevo por el teorema 2 tenemos que $[\alpha^{i+2\cdot\frac{p-1}{d}}, \alpha^{j+2\cdot\frac{p-1}{2}}]$ nos produce un polinomio de permutacion. Nuestro argumento es que este proceso se puede repetir a lo sumo $d-1$ veces. En la repeticion d obtenemos $[\alpha^{i+d\cdot\frac{p-1}{d}} = \alpha^i, \alpha^{j+d\cdot\frac{p-1}{2}} = \alpha^j]$. Por lo tanto por cada par $[a, b]$, obtenemos un conjunto de d pare tal que cada par nos produce un polinomio de permutacion: $\left\{[\alpha^i, \alpha^j], [\alpha^{i+\frac{p-1}{d}}, \alpha^{j+\frac{p-1}{2}}], [\alpha^{i+2\cdot\frac{p-1}{d}}, \alpha^{j+2\cdot\frac{p-1}{2}}], \cdots, [\alpha^{i+(d-1)\cdot\frac{p-1}{d}}, \alpha^{j+(d-1)\cdot\frac{p-1}{2}}]\right\}$. Esto implica que la cantidad de pares es $n = d \cdot q, q \in \mathbb{N}$. Por lo tanto $d \mid n$. □