Frobenius linear translators giving rise to new infinite classes of permutations and bent functions

Nastja Cepak[1] Enes Pasalic [1] Amela Muratović-Ribić [2]

[1] University of Primorska, Koper, Slovenia
[2] University of Sarajevo, Sarajevo, Bosnia and Herzegovina

June 8, 2018

Motivation

The importance of permutations over finite fields in applications such as coding is well known.

Motivation

The importance of permutations over finite fields in applications such as coding is well known.

Especially useful are sparse permutations but finding their explicit form is difficult.

Motivation

The importance of permutations over finite fields in applications such as coding is well known.

Especially useful are sparse permutations but finding their explicit form is difficult.

In a previous work by Cepak, Charpin, Pasalic [CCP], Gohar Kyureghyan's work was used to constructed new families of permutations that generalize many previously used approaches.

Motivation

The importance of permutations over finite fields in applications such as coding is well known.

Especially useful are sparse permutations but finding their explicit form is difficult.

In a previous work by Cepak, Charpin, Pasalic [CCP], Gohar Kyureghyan's work was used to constructed new families of permutations that generalize many previously used approaches.

The constructions relied on functions admitting **linear translators**.

Definitions

Linear translator

Let $n = rk$, $1 \leq k \leq n$. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and b fixed in $\mathbb{F}_{p^k}$. Then γ is a *b-linear translator* of f if

$$f(x + u\gamma) - f(x) = ub, \quad \text{for all } x \in \mathbb{F}_{p^n} \text{ and for all } u \in \mathbb{F}_{p^k}.$$

Definitions

Linear translator

Let $n = rk$, $1 \leq k \leq n$. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}^*_{p^n}$ and b fixed in $\mathbb{F}_{p^k}$. Then γ is a *b-linear translator* of f if

$$f(x + u\gamma) - f(x) = ub, \quad \text{for all } x \in \mathbb{F}_{p^n} \text{ and for all } u \in \mathbb{F}_{p^k}.$$

Linear structure

When $k = 1$, γ is usually said to be a *b-linear structure* of the function f (where $b \in \mathbb{F}_p$), that is

$$f(x + \gamma) - f(x) = b \;\text{ for all } x \in \mathbb{F}_{p^n}.$$

Linear translators

G.Kyureghyan, 2011

Let $n = rk$, with $r, k > 1$. Let L be a $\mathbb{F}_{p^k}$-linear permutation on $\mathbb{F}_{p^n}$, f a function from $\mathbb{F}_{p^n}$ onto $\mathbb{F}_{p^k}$, $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$, and b is fixed in $\mathbb{F}_{p^k}$. Assume that γ is a b-linear translator of f. Then

$$F(x) = L(x) + L(\gamma)h(f(x))$$

permutes $\mathbb{F}_{p^n}$ if and only if $g : u \mapsto u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

In [CCP] existence of linear translators in specific families of functions was considered. Results showed that **few types of functions admit a linear translator**.

In [CCP] existence of linear translators in specific families of functions was considered. Results showed that **few types of functions admit a linear translator**.

Proposition 1, [CCP]

Monomial functions $f(x) = x^d$ do not admit linear translators.

In [CCP] existence of linear translators in specific families of functions was considered. Results showed that **few types of functions admit a linear translator**.

Proposition 1, [CCP]

Monomial functions $f(x) = x^d$ do not admit linear translators.

Proposition 2, [CCP]

Let $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\beta \in \mathbb{F}_{p^n}^*$ and $n = rk$, where $r > 1$. Then the function f has a linear translator if and only if n is even, $k = \frac{n}{2}$, and furthermore $f(x) = T_k^n(x)$.

Solution is to

generalise the notion of linear translator!

.

Frobenius translators

Frobenius translator

Let $n = rk$, $1 \leq k \leq n$. Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and b fixed in $\mathbb{F}_{p^k}$. Then γ is an **(i, b)-Frobenius translator** for f if

$$f(x + u\gamma) - f(x) = u^{p^i} b \quad \text{for all } x \in \mathbb{F}_{p^n} \text{ and for all } u \in \mathbb{F}_{p^k},$$

where $i = 0, \ldots, k-1$.

G.Kyureghyan's construction Theorem was properly generalised to enable the use of Frobenius translators.

G.Kyureghyan's construction Theorem was properly generalised to enable the use of Frobenius translators.

Generalised Theorem

For $n = rk$, let $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an arbitrary mapping and let $\gamma \in \mathbb{F}_{p^n}$ be an (i, b)-Frobenius translator of $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, that is $f(x + u\gamma) - f(x) = u^{p^i} b$ for all $x \in \mathbb{F}_{p^n}$ and all $u \in \mathbb{F}_{p^k}$. Then, the mapping

$$G(x) = L(x)^{p^i} + L(\gamma)^{p^i} h(f(x)),$$

where $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is an F_{p^k}-linear permutation, permutes $\mathbb{F}_{p^n}$ if and only if the mapping $g(u) = u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

Example of functions admitting a Frobenius translator, but not a linear translator:

Let $p = 2$, $n = rk$ and $f : x \mapsto T_k^n(x^{2^{\ell k}+1})$ with $1 \leq \ell \leq r-1$. Let $\gamma \in \mathbb{F}$ and u be any element of $\mathbb{F}_{2^k}$.

Example of functions admitting a Frobenius translator, but not a linear translator:

Let $p = 2$, $n = rk$ and $f : x \mapsto T_k^n(x^{2^{\ell k}+1})$ with $1 \leq \ell \leq r-1$. Let $\gamma \in \mathbb{F}$ and u be any element of $\mathbb{F}_{2^k}$. Then

$$f(x) + f(x + u\gamma) \quad = \quad u \; T_k^n \left(x(\gamma^{2^{\ell k}} + \gamma^{2^{n-\ell k}}) \right) + u^2 \, T_k^n \left(\gamma^{2^{\ell k}+1} \right).$$

Example of functions admitting a Frobenius translator, but not a linear translator:

Let $p = 2$, $n = rk$ and $f : x \mapsto T_k^n(x^{2^{\ell k}+1})$ with $1 \leq \ell \leq r-1$. Let $\gamma \in \mathbb{F}$ and u be any element of $\mathbb{F}_{2^k}$. Then

$$f(x) + f(x + u\gamma) \;\; = \;\; u \; T_k^n \left(x(\gamma^{2^{\ell k}} + \gamma^{2^{n-\ell k}}) \right) + u^2 \, T_k^n \left(\gamma^{2^{\ell k}+1} \right).$$

If $\gamma^{2^{2\ell k}} = \gamma$ then $f(x) + f(x + u\gamma) = u^2 \; T_k^n(\gamma^{2^{\ell k}+1})$, for all x and all $u \in \mathbb{F}_{2^k}$.

In that case the function **DOES NOT admit a linear translator**, but it **DOES admit a Frobenius translator**.

Proposition

Let $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\beta \in \mathbb{F}_{p^n}^*$ and $n = rk$, where $r > 1$. Then the function f has a Frobenius translator γ if and only if n is even, and $k = \frac{n}{2}$. Furthermore, $f(x) = x^{p^{i'}} + x^{p^{i'+\frac{n}{2}}}$ and γ is an $(i', \gamma^{p^{i'}} + \gamma^{p^{i'+\frac{n}{2}}})$-Frobenius translator.

Proposition

Let $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\beta \in \mathbb{F}_{p^n}^*$ and $n = rk$, where $r > 1$. Then the function f has a Frobenius translator γ if and only if n is even, and $k = \frac{n}{2}$. Furthermore, $f(x) = x^{p^{i'}} + x^{p^{i'+\frac{n}{2}}}$ and γ is an $(i', \gamma^{p^{i'}} + \gamma^{p^{i'+\frac{n}{2}}})$-Frobenius translator.

The existence of larger families of **cubic** functions admitting translators is still an open problem!

Proposition

Let $f(x) = Tr_q^{q^n}(x^{p^i+p^j} + ax^{p^i+1})$, where $i > j$ and $q = p^m$. Then the function f has a Frobenius translator if and only if m divides j, j divides i, i divides n in such a way that we can write $q = p^m, j = bm, i = cj = cbm$, and $n = ri = rcbm$ for some integers b, c, r,

$$(\gamma^{p^{bm}} + a\gamma)^{p^r} + \gamma^{p^{cbm+rc}} + a\gamma^{p^{cbm}} = 0, \text{ and}$$

$$Tr_q^{q^n}(a\gamma^{q^{bc}+1} + \gamma^{q^{bc}+q^b}) \neq 0.$$

Frobenius translators also enabled generalisation of certain constructions of bent functions.

In Mesnager, 2014, constructions rely on existence of permutations satisfying the $\mathcal{A}_n$ property:

Frobenius translators also enabled generalisation of certain constructions of bent functions.

In Mesnager, 2014, constructions rely on existence of permutations satisfying the $\mathcal{A}_n$ property:

Three pairwise distinct permutations ϕ_1, ϕ_2, ϕ_3 of $\mathbb{F}_{2^n}$ are said to satisfy $(\mathcal{A}_n)$ if the following conditions hold:

- $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^n}$,
- $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

Frobenius translators also enabled generalisation of certain constructions of bent functions.

In Mesnager, 2014, constructions rely on existence of permutations satisfying the $\mathcal{A}_n$ property:

Three pairwise distinct permutations ϕ_1, ϕ_2, ϕ_3 of $\mathbb{F}_{2^n}$ are said to satisfy $(\mathcal{A}_n)$ if the following conditions hold:

- $\psi = \phi_1 + \phi_2 + \phi_3$ is a permutation of $\mathbb{F}_{2^n}$,
- $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

Using Forbenius translators the family of permutations satisfying these properties can be vastly expanded.

Generalisation of Proposition 3, [Mesnager, Ongan, Özbudak 2017]

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an $\mathbb{F}_{2^k}$-linear permutation of $\mathbb{F}_{2^n}$, and let $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation. Assume $\gamma \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^k}^*$ are such that γ is an (a, i)-Frobenius translator of f with respect to $\mathbb{F}_{2^k}$. Then the function $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$,

$$\phi = L(x) + L(\gamma)\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}},$$

is a permutation polynomial of $\mathbb{F}_{2^n}$ and

$$\phi^{-1} = L^{-1}(x) + \gamma a^{2^i}\left(g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right) + f(L^{-1}(x))\right)^{2^{n-i}}.$$

Generalisation of Theorem 1, [Mesnager, Ongan, Özbudak 2017]

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an $\mathbb{F}_{2^k}$-linear permutation of $\mathbb{F}_{2^n}$, and let $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation. Assume $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{2^n}^*$ are all pairwise distinct (a, i)-Frobenius translators of f with respect to $\mathbb{F}_{2^k}$ $(a \in \mathbb{F}_{2^k}^*)$ such that $\gamma_1 + \gamma_2 + \gamma_3$ is again an (a, i)-Frobenius translator.

Suppose $\gamma_1 + \gamma_2 + \gamma_3 \neq 0$. Set $\rho(x) = \left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}$ and

$\tilde{\rho}(x) = a^{2^i} \left(g^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)^{2^{n-i}}$.

Then,

$$\begin{aligned} H(x,y) &= Tr(xL(y)) + Tr(L(\gamma_1)x\rho(y))\,Tr(L(\gamma_2)x\rho(y)) + \\ &\quad Tr(L(\gamma_1)x\rho(y))\,Tr(L(\gamma_3)x\rho(y)) + \\ &\quad Tr(L(\gamma_2)x\rho(y))\,Tr(L(\gamma_3)x\rho(y)) \end{aligned}$$

is bent. Furthermore, its dual function H^* is given by

$$\begin{aligned} H^*(x,y) &= Tr(yL^{-1}(x)) + Tr(\gamma_1 y\tilde{\rho}(L^{-1}(x)))\,Tr(\gamma_2 y\tilde{\rho}(L^{-1}(x))) + \\ &\quad Tr(\gamma_1 y\tilde{\rho}(L^{-1}(x)))\,Tr(\gamma_3 y\tilde{\rho}(L^{-1}(x))) + \\ &\quad Tr(\gamma_2 y\tilde{\rho}(L^{-1}(x)))\,Tr(\gamma_3 y\tilde{\rho}(L^{-1}(x))). \end{aligned}$$

Thank you for your attention