New classes of permutations and secondary bent functions via Frobenius translators

N. Cepak*, E. Pasalic*, and A. Muratović-Ribić**

*IAM and FAMNIT, University of Primorska, Koper, Slovenia
**University of Sarajevo, Bosnia and Herzegovina

We show the existence of many explicitly defined infinite classes of permutations over finite fields by extending the notion of linear translators, introduced by Kyureghyan [3]. This paper essentially generalizes the results of two articles [1, 4].[1] In [1] several new classes of permutation polynomials of the form

$$F \; : \; x \mapsto L(x) + L(\gamma)h(f(x)), \tag{1}$$

where $f : \mathbb{F}_{p^{rk}} \to \mathbb{F}_{p^k}, h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}, \gamma \in \mathbb{F}^*_{p^{rk}}$ is a so-called *b-linear translator* of f and L a linear permutation, which were originally studied by Kyureghyan [3].

The main obstacle when considering permutations of the form (1) is that new classes of permutation polynomials could be specified provided the existence of suitable polynomials $\{f\}$ admitting linear translators. Such polynomials turns out to be quite rare [1] and we introduce *Frobenius translators* so that $f(x + u\gamma) - f(x) = u^{p^i}b$, for all $x \in \mathbb{F}_{p^n}$ and all $u \in \mathbb{F}_{p^k}$, whereas the standard definition covers only the case $i = 0$.

Theorem 0.1 *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*

$$G(x) = L(x)^{p^i} + L(\gamma)^{p^i} h(f(x)), \tag{2}$$

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 $g(u) = u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

To justify this extension we may for instance consider the mapping $f : x \mapsto T^n_k(x^{2^{\ell k}+1})$ over $\mathbb{F}_{2^n}$, where $n = rk, 1 \leq \ell \leq r - 1$, which does not have linear but admits a Frobenius translator. This gives us the possibility to construct permutation polynomials of the form

$$L(x)^{p^i} + L(\gamma)^{p^i} h(f(x)), \tag{3}$$

which greatly resembles (1) though Frobenius translators are used instead. For instance, among other results, we have:

Proposition 0.2 *For $n = 4k$, the function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{2k}}$, defined by $f(x) = Tr^n_k(x) + Tr^n_{2k}(x)$, always has a 0-translator if $\gamma + \gamma^{p^{2k}} = 0$. In the binary case, it also has a $(k, \gamma^{p^k} + \gamma^{p^{3k}})$-Frobenius translator.*

In connection to [1], we also present new classes of permutations of the form $F(x) = L(x) + (x^{p^k} - x + \delta)^s$.

Theorem 0.3 *Let p be odd, $n = 2k, \mathcal{S} = \{y \in \mathbb{F}_{p^n} \mid T^n_k(y) = 0\}, L$ be a linear permutation. Then $F(x) = L(x) + (x^{p^k} - x + \delta)^s$, is a permutation for any $\delta \in \mathcal{S}, s \in \{2, 4, \ldots, p^n - 1\}$, or for any $\delta \in \mathbb{F}_{p^n}, s = t(p^k + 1), t \in \mathbb{N}$.*

[1] The extended version of this abstract is available at https://arxiv.org/abs/1801.08460.

In the second part of this article, we consider the extension of Mesnager *et al.* [5, 6], where secondary bent functions are deduced using a suitable set of permutations constructed using linear translators. The method uses a quadruple of bent functions that satisfy certain property (called $(\mathcal{A}_n)$) , which can be suitably derived from permutations obtained using the concept of linear translators. These results are generalized in a straightforward manner using Frobenius translators, thus offering a wider class of secondary bent functions.

Theorem 0.4 (Generalized Theorem 1, [4]) *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,*

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

is bent.

The existence of pairwise distinct (a, i)-Frobenius translators $\gamma_1, \gamma_2, \gamma_3$ such that $\gamma_1 + \gamma_2 + \gamma_3$ is again an (a, i)-Frobenius translator is also confirmed.

The results in [2, 5, 6] and our generalization that is based on Frobenius translators consider quadruples of bent functions whose duals are related through $f_1^* + f_2^* + f_3^* + f_4^* = 0$. On the other hand, a recent initiative taken in [2] provides slightly different framework for designing secondary bent functions where instead the condition is that $f_1^* + f_2^* + f_3^* + f_4^* = 1$. The existence of such quadruples of bent functions was left as an open problem in [2].

Theorem 0.5 *Let $f_i(x, y) = Tr(x\phi_i(y)) + h_i(y)$ for $i \in \{1, 2, 3\}$, where ϕ_i satisfies the condition $(\mathcal{A}_n)$ and $x, y \in \mathbb{F}_{2^{n/2}}$. If the functions h_i satisfy*

$$\begin{aligned} h_1(\phi_1^{-1}(x)) + h_2(\phi_2^{-1}(x)) + h_3(\phi_3^{-1})(x))+ \\ (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(x)) = 1, \end{aligned}$$

then f_1, f_2, f_3 are solutions to Open Problem in [2].

The condition on h_i turns out to be easily specified and an example of construction is provided in the extended version.

References

[1] N. Cepak, P. Charpin, and E. Pasalic, *Permutations via linear translators.* Finite Fields and Their Applications., vol. 45, 2017, pp.19-42.

[2] S. Hodžić, E. Pasalic, and Y. Wei, *A general framework for secondary constructions of bent and plateaued functions.* Submitted manuscript.

[3] G.M. Kyureghyan, *Constructing permutations of finite fields via linear translators.* Journal of Combinatorial Theory, Series A 118, 2011, pp. 1052-1061.

[4] S. Mesnager, P. Ongan, and F. Özbudak, *New bent functions from permutations and linear translators.* C2SI 2017: Codes, Cryptology and Information Security, pp. 282-297.

[5] S. Mesnager, *Several new infinite families of bent functions and their duals.* IEEE Trans. Inf. Theory 60(7), 2014, pp. 4397-4407.

[6] S. Mesnager, P. Ongan, and F. Özbudak, *Further constructions of infinite families of bent functions from new permutations and their duals.* Cryptography and Communications 8.2, 2016, pp.229-246.