On Plateaued Functions, Linear Structures and Permutation Polynomials

Sihem Mesnager[1], Kübra Kaytancı[2], and Ferruh Özbudak[3](✉)

[1] LAGA, UMR 7539, CNRS, University Paris XIII - Sorbonne Paris Cité, University Paris VIII (Department of Mathematics) and Telecom ParisTech, Paris, France
smesnager@univ-paris8.fr

[2] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
kubra.kaytanci@metu.edu.tr

[3] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. We obtain concrete upper bounds on the algebraic immunity of a class of highly nonlinear plateaued functions without linear structures than the one was given recently in 2017, Cusick. Moreover, we extend Cusick's class to a much bigger explicit class and we show that our class has better algebraic immunity by an explicit example. We also give a new notion of linear translator, which includes the Frobenius linear translator given in 2018, Cepak, Pasalic and Muratović-Ribić as a special case. We find some applications of our new notion of linear translator to the construction of permutation polynomials. Furthermore, we give explicit classes of permutation polynomials over $\mathbb{F}_{q^n}$ using some properties of $\mathbb{F}_q$ and some conditions of 2011, Akbary, Ghioca and Wang.

Keywords: Plateaued functions · Linear structure · Permutation polynomials

1 Introduction

Plateaued functions are important not only for cryptography but also for some related areas including coding theory and communication. There have been many results in recent years regarding their construction, existence and applications. We refer for example to [2–6,10,14,16–19] and the references therein.

Recently Cusick [9] gave an explicit construction of highly nonlinear plateaued functions without linear structure. In Sect. 3 we obtain a much larger class of explicit functions having all these good properties and including Cusick's class of functions as a very small subclass. Moreover, we prove that Cusick's class have quite low algebraic immunity by concrete upper bounds. We also give an explicit example in our class having better algebraic immunity than the functions in Cusick's class.

C. Carlet et al. (Eds.): C2SI 2019, LNCS 11445, pp. 217–235, 2019.
https://doi.org/10.1007/978-3-030-16458-4_13

For construction of non-trivial mathematical structures it has been shown that linear structures (and linear translators) are useful. There are important connections between linear translators and permutation polynomials over finite fields (see, for example [11]). Recently the authors in [8] gave a generalization of linear translators, which they call the Frobenius linear translator. They also give applications of their generalization to the construction of permutation polynomials. In Sect. 6 we obtain a further and natural generalization of linear translators using additive polynomials. Our generalization also has applications to the construction of permutation polynomials using our generalization different from Frobenius linear translators (see, for example Theorems 5 and 6 and Example 2 below).

Akbary, Ghioca and Wang [1] established a very interesting method in order to construct permutation polynomials over "big" finite fields. If an explicit class of permutation polynomials that satisfies certain criteria is found over a subfield, $\mathbb{F}_q$ it can be used to construct an explicit class of permutation polynomials over an extension field $\mathbb{F}_{q^n}$. For example, the authors in [7] obtained such explicit permutation polynomial classes over $\mathbb{F}_{q^2}$ using certain properties of $\mathbb{F}_q$. By a similar motivation we obtain further explicit permutation polynomial classes over $\mathbb{F}_{q^2}$ via $\mathbb{F}_q$ and also over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 3$ in Sects. 4 and 5, respectively.

We give details of our corresponding contributions and motivations in the beginnings of Sects. 3, 4, 5 and 6 below. We give some background in the next section.

2 Preliminaries

Let q be a power of a prime number and $\mathbb{F}_{q^n}$ be the finite field of order q^n where $n \geq 1$. The extension field $\mathbb{F}_{q^n}$ can be viewed as an n-dimensional vector space over $\mathbb{F}_q$. The trace function Tr_n from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined as

$$\begin{aligned} Tr_n : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}. \end{aligned}$$

A Boolean function f of n-variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

Definition 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then the Walsh transform $\hat{f}$ of f is defined as*

$$\begin{aligned} \hat{f} : \mathbb{F}_2^n &\to \mathbb{Z} \\ w &\mapsto \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + w \cdot x} \end{aligned}$$

where $w = (w_1, w_2, \ldots, w_n)$, $x = (x_1, x_2, \ldots, x_n)$ and $w \cdot x = w_1 x_1 + \cdots + w_n x_n$.

Definition 2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f has linear structure at $a \in \mathbb{F}_2^n$ if and only if either $f(x+a) + f(x) = 0$ for any $x \in \mathbb{F}_2^n$(a is called a 0-linear structure) or $f(x+a) + f(x) = 1$ for any $x \in \mathbb{F}_2^n$(a is called a 1-linear structure).*

Definition 3. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f is called an s-plateaued function where $0 \leq s \leq n$ if $|\hat{f}(w)|^2 \in \{0, 2^{n+s}\}$ for any $w \in \mathbb{F}_2^n$.*

Definition 4 (See, for example [3]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The algebraic normal form of f is*

$$f(x) = \bigoplus_{\mathcal{I} \in \mathcal{P}(N)} a_{\mathcal{I}} \left(\prod_{\mathcal{I} \in \mathcal{P}(N)} x^{\mathcal{I}} \right),$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, \ldots, n\}$. The degree of the algebraic normal form of f is equal to

$$\max\{|\mathcal{I}| : a_{\mathcal{I}} \neq 0\}$$

where $|\mathcal{I}|$ denotes the size of $\mathcal{I}$.

Definition 5 (See, for example [3]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}$ be a Boolean function. The algebraic immunity $AI(f)$ of f is defined to be the minimal degree of a nonzero function g from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for which $f \cdot g = 0$ or $(f+1) \cdot g = 0$, i.e*

$$AI(f) := min\{\deg g : g \in Ann(f) \cup Ann(f+1)\}$$

where $Ann(f)$ is the set of annihilators of f. A function g is an annihilator of f if $f \cdot g = 0$.

Remark 1. It is well-known that for any Boolean function f of n-variables, $AI(f) \leq \lceil \frac{n}{2} \rceil$.

For integer $n \geq 1$ and $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, the inner product $x \cdot y \in \mathbb{F}_2$ is the usual inner product defined as

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

3 Cusick's Highly Nonlinear Plateaued Functions and Their Modifications

For integers $d \geq 3$ and $k \geq 1$, Cusick introduced an explicit class of Boolean functions of degree d in $n = 2dk - 1$ variables given by

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{j=0}^{k-1} x_{dj+1} \ldots x_{dj+d} + \sum_{j=1}^{m-1} x_j x_{j+m}. \tag{1}$$

where $m = dk$. He proved that these are 1-plateaued, have no linear structure and have nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$. They become balanced by adding a concrete linear function. Note that adding a linear function does not change plateauedness, nonlinearity or the set of linear structures. He also states that "... a high algebraic immunity is not to be expected" in [9, page 80, the last paragraph].

In this section we show that indeed algebraic immunity of the functions in (1) is low. Note that the largest degree of the class for a fixed odd integer $n \geq 3$ occurs when $k = 1$. Moreover, if $m = \frac{n-1}{2}$ is a prime, then k may only taken to be 1 in (1). The following result shows in particular that this class has very low algebraic immunity when k is small.

Proposition 1. *For integers $d \geq 3$ and $k \geq 1$, let $n = 2dk - 1$ and $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ be the Boolean function defined in (1). We have:*

(i) $AI(f_1) \leq 3$.
(ii) For $k \geq 2$, $AI(f_k) \leq \min\{k + 2, \frac{n+1}{2k}\}$.

Proof. We first prove item (i). Put $x = (x_1, x_2, \dots, x_{m-1})$ and $y = (y_1, \dots, y_{m-1}) = (x_{m+1}, \dots, x_{2m-1})$ where $m = dk$. Let

$$h(x) = x_1x_2 \dots x_{m-1} \text{ and } g(x, y) = x_1y_1 + x_2y_2 + \dots + x_{m-1}y_{m-1}.$$

Then it is easy to observe that

$$f_1(x_1, \dots, x_n) = h(x)x_m + g(x, y).$$

It is enough to prove that

$$f_1(x_1, \dots, x_n)\,(g(x, y) + 1)\,(x_m + 1) = 0$$

for all $x, y \in \mathbb{F}_2^{m-1}$ and $x_m \in \mathbb{F}_2$. Indeed, $\deg\,(g(x, y) + 1)\,(x_m + 1) = 2 + 1 = 3$. Moreover,

$$\begin{aligned} f_1(x_1, \dots, x_n)\,(g(x, y) + 1)\,(x_m + 1) &= (h(x)x_m + g(x, y))\,(g(x, y) + 1)\,(x_m + 1) \\ &= (h(x)x_mg(x, y) + h(x)x_m + g(x, y) + g(x, y))\,(x_m + 1) \\ &= (h(x)x_m\,(g(x, y) + 1))\,(x_m + 1) \\ &= h(x)\,(g(x, y) + 1)\,(x_m(x_m + 1)) = 0, \end{aligned}$$

as $(x_m(x_m + 1)) = 0$. This completes the proof of item (i).

Next, we consider the proof of item (ii). Note that

$$f_k(x_1, \dots, x_n) = x_1 \dots x_d + x_{d+1} \dots x_{2d} + \dots + x_{(k-1)(d+1)} \dots x_{m-1}x_m + g(x, y).$$

Here

$$\begin{aligned} f_k(x_1, \dots, x_n)\,&\big((x_1 + 1)(x_d + 1) \dots (x_{(k-1)(d+1)} + 1\big)\,(g(x, y) + 1)) \\ &= x_1(x_1 + 1)r_1(x_1, \dots, x_n) + x_{d+1}(x_{d+1} + 1)r_2(x_1, \dots, x_n) + \dots \\ &+ x_{(k-1)(d+1)}(x_{(k-1)(d+1)} + 1)r_k(x_1, \dots, x_n) \\ &+ g(x, y)\,(g(x, y) + 1)\,r_{k+1}(x_1, \dots, x_n) \end{aligned}$$

for some polynomials $r_1(x_1, \dots, x_n), \dots, r_{k+1}(x_1, \dots, x_n)$ in algebraic normal form. As

$$x_1(x_1 + 1) = x_{d+1}(x_{d+1} + 1) = \dots = x_{(k-1)(d+1)}(x_{(k-1)(d+1)} + 1) = 0$$

and $g(x,y)\,(g(x,y)+1)=0$ as Boolean functions and

$$\deg\big((x_1+1)(x_{d+1}+1)\dots(x_{(k-1)(d+1)}+1)\,(g(x,y)+1)\big)=k+2,$$

we have $AI(f_k)\le k+2$. Also

$$f_k(x_1,\dots,x_n)\,(f_k(x_1,\dots,x_n)+1)=0.$$

And $\deg(f_k(x_1,\dots,x_n)+1)=d=\frac{n+1}{2k}$. Hence $AI(f_k)\le\min\{k+2,\frac{n+1}{2k}\}$. □

Next, we define a much larger explicit class of Boolean functions containing Cusick's class as defined in (1) as a small subclass. The functions of this class are 1-plateaued, having nonlinearity $2^{n-1}-2^{\frac{n-1}{2}}$ and balanced up to addition of a concrete linear function as in Cusick's class. Moreover, we also have a characterization whether a function in our class has a linear structure. This condition is easy to apply. Moreover, we give an explicit example demonstrating that the algebraic immunity of a function in our class is much better compared to the class defined in (1).

We first note that if $h:\mathbb{F}_2^{m-1}\to\mathbb{F}_2$ is an arbitrary map, then we have

$$|\{(\alpha_m,\beta)\in\mathbb{F}_2\times\mathbb{F}_2^{m-1}:h(\beta)+\alpha_m=0\}|=2^{m-1}.$$

Now we are ready to give our much larger class of Boolean functions consisting of 1-plateaued, highly nonlinear functions without linear structure. It is easy to make them balanced by adding a linear term as explained in the theorem as well.

Theorem 1. *Let $n\ge 3$ be odd and $n=2m-1$. Let $\pi:\mathbb{F}_2^{m-1}\to\mathbb{F}_2^{m-1}$ be a permutation map. Let $g_0,g_1:\mathbb{F}_2^{m-1}\to\mathbb{F}_2$ be Boolean maps. Let $f:\mathbb{F}_2^n\to\mathbb{F}_2$ be the Boolean map defined as*

$$\begin{aligned}f:\mathbb{F}_2^{m-1}\times\mathbb{F}_2\times\mathbb{F}_2^{m-1}&\to\mathbb{F}_2\\ (x,x_m,y)&\mapsto g_0(x)+x_mg_1(x)+\pi(x)\cdot y.\end{aligned}$$

Then we have:

(i) f is a 1-plateaued function.

(ii) f has no nonzero linear structure if and only if the subset

$$S=\{(\alpha_m,\beta)\in\mathbb{F}_2\times\mathbb{F}_2^{m-1}:g_1(\pi^{-1}(\beta))+\alpha_m=0\}\subseteq\mathbb{F}_2\times\mathbb{F}_2^{m-1}$$

is not an affine or linear subset (of dimension m-1).

(iii) The nonlinearity of f is $2^{n-1}-2^{(n-1)/2}$.

(iv) For $(u,\mu,v)\in\mathbb{F}_2^{m-1}\times\mathbb{F}_2\times\mathbb{F}_2^{m-1}$, the function

$$f_{u,\mu,v}(x,x_m,y):=f(x,x_m,y)+u\cdot x+\mu\cdot x_m+v\cdot y$$

is balanced if and only if $g_1(\pi^{-1}(v))+\mu=1$.

Proof. Let $w = (\alpha, \alpha_m, \beta) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$. We have

$$\begin{aligned}\hat{f}(w) &= \sum_{x \in \mathbb{F}_2^{m-1}} \sum_{x_m \in \mathbb{F}_2} \sum_{y \in \mathbb{F}_2^{m-1}} (-1)^{g_0(x)+x_m g_1(x)+\pi(x)\cdot y+\alpha\cdot x+\alpha_m x_m+\beta\cdot y} \\ &= \sum_{x \in \mathbb{F}_2^{m-1}} \sum_{x_m \in \mathbb{F}_2} (-1)^{g_0(x)+x_m g_1(x)+\alpha\cdot x+\alpha_m x_m} \sum_{y \in \mathbb{F}_2^{m-1}} (-1)^{(\pi(x)+\beta)\cdot y} \\ &= 2^{m-1}(-1)^{g_0(\pi^{-1}(\beta))+\alpha\cdot\pi^{-1}(\beta)} \sum_{x_m \in \mathbb{F}_2} (-1)^{(g_1(\pi^{-1}(\beta))+\alpha_m)x_m}.\end{aligned}$$

Hence

$$\hat{f}(w) = \begin{cases} 2^m(-1)^{g_0(\pi^{-1}(\beta))+\alpha\cdot\pi^{-1}(\beta)} & \text{if } g_1(\pi^{-1}(\beta)) = \alpha_m, \\ 0 & \text{otherwise.} \end{cases}$$

This completes the proof of the item (i).

It is well-known that the nonlinearity of an arbitrary Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is $2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |\hat{f}(w)|$. Hence in our case the nonlinearity of our function f is

$$2^{n-1} - \frac{1}{2} \max_{w \in \mathbb{F}_2^n} |\hat{f}(w)| = 2^{n-1} - \frac{1}{2} 2^m = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

This completes the proof of item (iii).

It is also well-known that the Walsh value $\hat{f}_{u,\mu,v}(0,0,0)$ of $\hat{f}_{u,\mu,v}(x, x_m, y)$ is $\hat{f}(u, \mu, v)$. Hence

$$\hat{f}_{u,\mu,v}(0,0,0) = 0 \Longleftrightarrow g_1(\pi^{-1}(v)) + \mu = 1.$$

Note that $f_{u,\mu,v}(x, x_m, y)$ is balanced if and only if $\hat{f}_{u,\mu,v}(0,0,0) = 0$. This completes the proof of item (iv).

It only remains to prove the item (ii). Let S_f denote the support of the Walsh spectrum of f, that is $S_f = \{w \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : \hat{f}(w) \neq 0\}$. Let $S \subseteq \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ be the subset defined as

$$S = \{(\alpha_m, \beta) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : g_1(\pi^{-1}(\beta)) + \alpha_m = 0\}. \tag{2}$$

It follows from the proof of item (i) above that $S_f = \mathbb{F}_2^{m-1} \times S$. For $\nu \in \mathbb{F}_2^n$, let $\Delta_f(\nu)$ be the sum

$$\Delta_f(\nu) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x+\nu)+f(x)}.$$

It is clear that ν is a linear structure of f if and only if $\Delta_f(\nu) = \pm 2^n$. Moreover, it is not difficult to observe that

$$\sum_{w \in \mathbb{F}_2^n} \hat{f}(w)^2 (-1)^{\nu\cdot w} = 2^n \Delta_f(\nu),$$

which holds for an arbitrary Boolean map $f : \mathbb{F}_2^n \to \mathbb{F}_2$. In our case f is 1-plateaued and hence

$$\sum_{w\in\mathbb{F}_2^n} \hat{f}(w)^2(-1)^{\nu\cdot w} = \sum_{w\in S_f} |\hat{f}(w)|^2(-1)^{\nu\cdot w} = 2^{n+1}\sum_{w\in S_f}(-1)^{\nu\cdot w},$$

where we use our proof of item (i) above. These implies that if $\nu \in \mathbb{F}_2^n$, then we have

$$\varDelta_f(\nu) = 2\sum_{w\in S_f}(-1)^{\nu\cdot w}.$$

As $|S_f| = 2^{n-1}$, we conclude that $\nu \in \mathbb{F}_2^n$ is a linear structure of f if and only if ($\nu \cdot w = 0$ for all $w \in S_f$) or ($\nu \cdot w = 1$ for all $w \in S_f$). Assume that $v = (a, a_m, b) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ is a nonzero linear structure of f. Recall that $S_f = \mathbb{F}_2^{m-1} \times S$ where S is defined in (2). First we show that $a = 0$. Indeed otherwise there exist $\alpha, \alpha' \in \mathbb{F}_2^{m-1}$ such that $a\cdot\alpha \neq a\cdot\alpha'$. For fixed $(\alpha_m, \beta) \in S$, both $(\alpha, \alpha_m, \beta)$ and $(\alpha', \alpha_m, \beta)$ are elements of S_f. Then it is impossible that $(a, a_m, b)\cdot(\alpha, \alpha_m, b) = (a, a_m, b)\cdot(\alpha', \alpha_m, b)$ which is a contradiction.

Next, assume that $\nu \cdot w = 0$ for all $w \in S_f$. Then $\nu = (0, a_m, b)$ and $0 = (a_m, b)\cdot(\alpha_m, \beta)$ for all $(\alpha_m, \beta) \in S$. As $\nu \neq 0$, there exist $(c, d) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ such that $(a_m, b)\cdot(c, d) \neq 0$. We choose such $(c, d) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$. As S is not a linear space and its cardinality is 2^{m-1}, the $\mathbb{F}_2$-span of S is the whole vector space $\mathbb{F}_2 \times \mathbb{F}_2^{m-1}$. In particular, there exist a subset $T \subseteq S$ such that

$$(c, d) = \sum_{(\alpha_m,\beta)\in T}(\alpha_m, \beta).$$

Multiplying both sides by (a_m, b) (as inner product) we get

$$(a_m, b)\cdot(c, d) = \sum_{(\alpha_m,\beta)\in T}(a_m, b)\cdot(c, d) = \sum_{(\alpha_m,\beta)\in T} 0 = 0.$$

However, this is a contradiction as $(a_m, b)\cdot(c, d) \neq 0$ by definition. This completes the proof of item (ii) under the assumption about $\nu \cdot w = 0$ for all $w \in S_f$.

Assume finally that $\nu \cdot w = 1$ for all $w \in S$. We choose $(\alpha_m^{(0)}, \beta^{(0)}) \in S$ and we define

$$S^L = \{(\alpha_m + \alpha_m^{(0)}, \beta + \beta^{(0)}) : (\alpha_m, \beta) \in S\}.$$

Note that S is affine if and only if S^L is linear. Moreover, $\nu = (0, a_m, b)$ is a nonzero linear structure of f if and only if $(a_m, b)\cdot(\alpha_m^L, \beta^L) = 0$ for all $(\alpha_m^L, \beta^L) \in S^L$. The same argument we used in the assumption $\nu \cdot w = 0$ for all $w \in S_f$ applied to S^L completes the proof. □

Example 1. Let $n = 2m - 1 = 11$. Choose the permutation map

$$\pi : \mathbb{F}_2^5 \longrightarrow \mathbb{F}_2^5$$
$$x = (x_0, x_1, x_2, x_3, x_4) \mapsto (\pi_1(x), \pi_2(x), \pi_3(x), \pi_4(x), \pi_5(x))$$

where

$$\begin{aligned}
\pi_1(x) &= x_0x_1x_2 + x_0x_1x_4 + x_0x_2x_3 + x_0x_2x_4 + x_0x_3 + x_0 + x_1x_2x_3x_4 + x_1x_2x_4\\
&\quad + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4,\\
\pi_2(x) &= x_0x_1x_2 + x_0x_1 + x_0x_2x_3x_4 + x_0x_2x_3 + x_0x_3x_4 + x_0x_3 + x_0x_4 + x_1x_2x_3\\
&\quad + x_1x_3x_4 + x_1x_4 + x_1 + x_2x_3 + x_3x_4,\\
\pi_3(x) &= x_0x_1x_3x_4 + x_0x_1x_3 + x_0x_1x_4 + x_0x_2x_4 + x_0x_2 + x_0x_3x_4 + x_1x_2x_3 + x_1x_2\\
&\quad + x_1x_3x_4 + x_1x_4 + x_2x_3x_4 + x_2 + x_3x_4,\\
\pi_4(x) &= x_0x_1x_2x_4 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_4 + x_0x_1 + x_0x_2x_4 + x_0x_2 + x_0x_3\\
&\quad + x_0 + x_1x_2x_4 + x_1x_3 + x_2x_3x_4 + x_2x_3 + x_3,\\
\pi_5(x) &= x_0x_1x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_4 + x_0x_2x_3 + x_0x_3x_4 + x_0x_3 + x_0x_4\\
&\quad + x_1x_2x_3 + x_1x_2x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1 + x_2x_4 + x_3x_4 + x_4.
\end{aligned}$$

Then take

$$\begin{aligned}
g_0 : \mathbb{F}_2^5 &\to \mathbb{F}_2\\
(x_0, x_1, x_2, x_3, x_4) &\mapsto x_0 + x_2 + x_3
\end{aligned}$$

and

$$\begin{aligned}
g_1 : \mathbb{F}_2^5 &\to \mathbb{F}_2\\
(x_0, x_1, x_2, x_3, x_4) &\mapsto x_1x_2x_3 + 1.
\end{aligned}$$

An application of our construction in Theorem 1 gives the map

$$\begin{aligned}
f : \mathbb{F}_2^5 \times \mathbb{F}_2 \times \mathbb{F}_2^5 &\to \mathbb{F}_2\\
(x, x_5, y) &\mapsto g_0(x) + x_5g_1(x) + \pi(x)y\\
(x_0, x_1, x_2, x_3, x_4, x_5, y_0, y_1, y_2, y_3, y_4) &\mapsto x_0 + x_2 + x_3 + (x_1x_2x_3 + 1)x_5 + y_0\pi_1(x)\\
&\quad + y_1\pi_2(x) + y_2\pi_3(x) + y_3\pi_4(x) + y_4\pi_5(x)
\end{aligned}$$

where $\pi_i(x)$ is defined as before for $i = 1, \ldots, 5$. The map is balanced, has no linear structure, has nonlinearity $992 = 2^{10} - 2^5$ and has algebraic immunity 4.

In Example 1, $\pi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ corresponds to the permutation map $x \mapsto x^{30}$. Note that as $m = 5$ is a prime, there is only one function in Cusick's class, which is f_1 in (1). Moreover, $AI(f_1) \leq 3$. Example 1 gives a concrete example in our class of Theorem 1 improving the algebraic immunity while keeping all the good properties of the maps of Cusick's class: high nonlinearity, 1-plateauedness, absence of having nonzero linear structures, and balancedness. Moreover, using different permutations $\pi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ and other suitable maps $g_0(x)$, $g_1(x)$ we get a lot of different Boolean functions with algebraic immunity 4 easily satisfying the conditions: 1-plateauedness, absence of having nonzero linear structures, and balancedness.

4 Constructing Permutation Polynomials over $\mathbb{F}_{q^2}$ via $\mathbb{F}_q$

Akbay, Ghioca and Wang [1] recently established a very interesting construction in order to construct polynomials over "big" finite fields using a commutative diagram relating the big field to some smaller subsets and the corresponding conditions on the maps of the commutative diagram. In fact, this construction gives different methods using different commutative diagrams leading to different conditions on different maps and subsets (see, for example [1, Proposition 5.9] and [1, Proposition 5.6]).

They generalized many earlier results and constructed many new permutation polynomial families. They also motivated many research directions in constructing explicit classes of permutation polynomials in "big" finite fields in the following sense: If a class of objects satisfying certain properties can be constructed which are guaranteed to satisfy a full set of conditions of Akbay, Ghioca and Wang in a small set (see, for example [1, Proposition 5.9] or [1, Proposition 5.6]), then it is possible to obtain an explicit class of permutation polynomials in the big finite field.

Recently Cepak, Charpin and Pasalic, among other results, gave such explicit classes in [7]. Namely, in [7, Section 6], they obtain permutation polynomials over $\mathbb{F}_{q^2}$ using certain polynomials over $\mathbb{F}_q$. We refer to Propositions 6, 8, 9 and the corresponding corollaries in [7].

Motivated by these results, we give explicit large class of permutation polynomials over $\mathbb{F}_{q^2}$ starting from polynomials over $\mathbb{F}_q$. We first introduce the notion of b-permutation.

Definition 6. *Let $m(x) \in \mathbb{F}_q[x]$ and $b \in \mathbb{F}_q$ be given. We call $m(x)$ a b-permutation over $\mathbb{F}_q$ if the evaluation mapping $x \mapsto m(x) + bx$ defines a permutation over $\mathbb{F}_q$.*

Remark 2. Note that it is not difficult to construct a b-permutation polynomial starting from a permutation polynomial. Indeed if $x \mapsto h(x)$ is a permutation polynomial, then $x \mapsto h(x) - bx$ is a b-permutation over $\mathbb{F}_q$.

First we present our results in characteristic 2. The following proposition indicates that it is easy to construct the corresponding large families of permutation polynomials over $\mathbb{F}_{q^2}$ as the component $g_0(x) \in \mathbb{F}_q[x]$ may be chosen arbitrarily.

Proposition 2. *Let $q = 2^k$ for some integer k. Let $\theta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ satisfy $\theta^q + \theta = 1$ and $g_0(x) \in \mathbb{F}_q[x]$ be arbitrary. Then we have:*

- *$F(x) = x + g_0(x^q + x) + \theta(x^{2^i q} + x^{2^i} + x^q + x)$ is a permutation over $\mathbb{F}_{q^2}$ for any $i \geq 1$.*
- *If $q \not\equiv 1 \mod 3$, then*

$$F(x) = x + g_0(x^q + x) + \theta(x^{3q} + x^{2q+1} + x^{q+2} + x^3 + x^q + x)$$

is a permutation over $\mathbb{F}_{q^2}$.

- *If* $q \not\equiv 1 \mod 5$, *then*

$$F(x) = x + g_0(x^q + x) + \theta(x^{5q} + x^{4q+1} + x^{q+4} + x^5 + x^q + x)$$

  is a permutation over $\mathbb{F}_{q^2}$.
- *If* $r \geq 1$ *is an integer such that* $\gcd(r, q-1) = 1$, *then*

$$F(x) = x + g_0(x^q + x) + \theta\left((x^q + x)^r + (x^q + x)\right)$$

  is a permutation over $\mathbb{F}_{q^2}$.

In fact, Proposition 2 is just a special subcase of the next theorem. We prefer to state Proposition 2 independently as it shows that the conditions of the next theorem are very easy to satisfy. We do not prove it as it follows from the proof of the next theorem.

Theorem 2. *Let* $q = 2^k$ *for some integer* k. *Let* $\theta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *satisfying* $\theta^q + \theta = 1$. *Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary and* $g_1(x) \in \mathbb{F}_q[x]$ *be a* 1*-permutation over* $\mathbb{F}_q$. *Then*

$$F(x) = x + g_0(x^q + x) + \theta(g_1(x^q + x))$$

is a permutation over $\mathbb{F}_{q^2}$.

Proof. The proof comes from [1, Proposition 5.9], by taking $g(x)$ of the form $g(x) = g_0(x) + \theta g_1(x) \in \mathbb{F}_{q^2}[x]$, $h(x)$ as a constant function equal to 1 and $\varphi(x) = x$. Observe that $S = \{y^q + y | y \in \mathbb{F}_{q^2}\} = \mathbb{F}_q$ since $\mathrm{char}(\mathbb{F}_q) = 2$. Then

$$h(x)\varphi(x) + g(x)^q + g(x) = x + g_0(x)^q + \theta^q g_1(x)^q + g_0(x) + \theta g_1(x).$$

If $x \in \mathbb{F}_q$, the equality implies

$$h(x)\varphi(x) + g(x)^q + g(x) = x + g_1(x).$$

Since $g_1(x)$ is a 1-permutation over $\mathbb{F}_q$, the function

$$F(x) = x + g_0(x^q + x) + \theta(g_1(x^q + x))$$

is a permutation over $\mathbb{F}_{q^2}$. □

Next, we present our results in odd characteristic. Again, we first state a special subcase in the next proposition.

Proposition 3. *Let* $q = p^k$, *where* p *is any odd prime number. Let* $\beta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *and* $\gamma = \beta^q - \beta$. *Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary. Then we have:*

- *If* $q \not\equiv 1 \mod 3$, *then*

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta\left[\frac{x^{3q}}{\gamma^{3q}} - 3\frac{x^{2q+1}}{\gamma^{2q+1}} + 3\frac{x^{q+2}}{\gamma^{q+2}} - \frac{x^3}{\gamma^3} - \frac{x^q}{\gamma^q} + \frac{x}{\gamma}\right]$$

  is a permutation over $\mathbb{F}_{q^2}$.

- *If* $q \not\equiv 1 \mod 5$, *then*

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)$$
$$+\beta\left[\frac{x^{5q}}{\gamma^{5q}} - 5\frac{x^{4q+1}}{\gamma^{4q+1}} + 10\frac{x^{3q+2}}{\gamma^{3q+2}} - 10\frac{x^{2q+3}}{\gamma^{2q+3}} + 5\frac{x^{q+4}}{\gamma^{q+4}} - \frac{x^5}{\gamma^5} - \frac{x^q}{\gamma^q} + \frac{x}{\gamma}\right]$$

is a permutation over $\mathbb{F}_{q^2}$.

- *If* $r \geq 1$ *is an integer such that* $\gcd(r, q-1) = 1$, *then*

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta\left[\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)^r - \left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)\right]$$

is a permutation over $\mathbb{F}_{q^2}$.

We do not prove Proposition 3 as its proof follows from the next theorem.

Theorem 3. *Let* $q = p^k$, *where* p *is any odd prime number. Let* $\beta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *and* $\gamma = \beta^q - \beta$. *Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary and* $g_1(x) \in \mathbb{F}_q[x]$ *be a 1-permutation over* $\mathbb{F}_q$. *Then*

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta g_1\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)$$

is a permutation over $\mathbb{F}_{q^2}$.

Proof. The proof comes from [1, Proposition 5.9], by taking $g(x)$ of the form $g(x) = g_0\left(\frac{x}{\gamma}\right) + \beta g_1\left(\frac{x}{\gamma}\right) \in \mathbb{F}_{q^2}[x]$, $h(x)$ as a constant function equal to 1 and $\varphi(x) = x$. Observe that $S = \{y^q - y | y \in \mathbb{F}_{q^2}\} = \gamma\mathbb{F}_q$. Now consider the map

$$\gamma y \mapsto \gamma y + g(\gamma y)^q - g(\gamma y).$$

Then

$$\begin{aligned}\gamma y + g(\gamma y)^q - g(\gamma y) &= \gamma y + g_0(y)^q + \beta^q g_1(y)^q - g_0(y) - \beta g_1(y)\\ &= \gamma y + (\beta^q - \beta)g_1(y)\\ &= \gamma[y + g_1(y)].\end{aligned}$$

Since $g_1(y)$ is a 1-permutation over $\mathbb{F}_q$, the function

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta g_1\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)$$

is a permutation over $\mathbb{F}_{q^2}$. □

5 Constructing Permutation Polynomials over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 3$

In Sect. 4 we give explicit classes of permutation polynomials over $\mathbb{F}_{q^2}$ using polynomials over $\mathbb{F}_q$.

In this section we give explicit classes of permutation polynomials over $\mathbb{F}_{q^n}$ using polynomials over $\mathbb{F}_q$ with $n \geq 3$. In fact, it is not easy to give such classes using the conditions of Akbary, Ghioca and Wang [1, Proposition 5.9] since we need to consider the subset $S = \{y^{q^n} - y | y \in \mathbb{F}_{q^n}\}$. This subset is easy to handle if $n = 2$, which we applied in Sect. 4. Hence in this section we use a different method of Akbary, Ghioca and Wang, namely [1, Proposition 5.6].

First we present our result for $n = 3$. The next proposition indicates the corresponding permutation polynomial class is large as the chosen components $g_1, g_2 \in \mathbb{F}_q[x]$ are arbitrary and $g_0 \in \mathbb{F}_q[x]$ has to satisfy a certain condition.

Proposition 4. *Let $\{\theta_0, \theta_1, \theta_2\}$ be a basis of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. We assume that $Tr_3(\theta_0) \neq 0$ without loss of generality. We choose $a_0, a_1, a_2 \in \mathbb{F}_q$ satisfying*

$$(a_0 - a_2)^2 + (a_2 - a_0)(a_1 - a_2) + (a_1 - a_2)^2 \neq 0. \tag{3}$$

Let $g_0, g_1, g_2 \in \mathbb{F}_q[x]$ be such that $g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2)$ is an $(a_0 + a_1 + a_2)$-permutation of $\mathbb{F}_q$. Then

$$F(x) = a_0x + a_0x^q + a_2x^{q^2} + \theta_0 g_0(Tr_3(x)) + \theta_1 g_1(Tr_3(x)) + \theta_2 g_2(Tr_3(x))$$

is a permutation over $\mathbb{F}_{q^3}$.

Proof. We use [1, Proposition 5.6], by taking $g(x)$ of the form

$$g(x) = \theta_0 g_0(x) + \theta_1 g_1(x) + \theta_2 g_2(x)$$

and $h(x)$ as a constant function equal to 1. Let $\varphi(x) = a_0x + a_1x^q + a_2x^{q^2} \in \mathbb{F}_q[x]$ with a_0, a_1, a_2 satisfying (3). For $x \in \mathbb{F}_q$ we have

$$\begin{aligned}\varphi(x) + Tr_3(g(x)) &= a_0x + a_1x^q + a_2x^{q^2} + Tr_3(\theta_0 g_0(x) + \theta_1 g_1(x) + \theta_2 g_2(x)) \\ &= (a_0 + a_1 + a_2)x + g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2).\end{aligned}$$

Since $g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2)$ is an $(a_0 + a_1 + a_2)$-permutation of $\mathbb{F}_q$, the condition (ii) of [1, Proposition 5.6] is satisfied.

It remains to prove that $\ker \varphi \cap \ker Tr_3 = \{0\}$. As $Tr_3(x) = x + x^q + x^{q^2}$ and $\varphi(x) = a_0x + a_1x^q + a_2x^{q^2} \in \mathbb{F}_q[x]$ considering their q-associates (see, for example, [13, Definition 3.58]) it is enough to prove that

$$\gcd(1 + t + t^2, a_0 + a_1t + a_2t^2) = 1. \tag{4}$$

Indeed, if follows from [13, Theorem 3.62] that $\ker \varphi \cap \ker Tr_3 = \{0\}$ if and only if (4) holds. By a simple computation we observe that (3) is equivalent to the condition

$$\gcd(1 + t + t^2, a_0 + a_1t + a_2t^2) = 1.$$

□

For $n \geq 3$ in general, the condition

$$(a_0 - a_2)^2 + (a_2 - a_0)(a_1 - a_2) + (a_1 - a_2)^2 \neq 0$$

corresponds to the resultant condition, which is well-known in algebraic geometry. We recall its definition (see, for example, [13, Definition 1.93]).

Definition 7. *Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ be a polynomial of degree n and $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in \mathbb{F}_q[x]$ be a polynomial of degree m with $n, m \in \mathbb{N}^+$. Then the resultant $Res(f, g)$ of the two polynomials is defined by the determinant*

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & & \dots & a_n \\ b_0 & b_1 & \dots & & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & & b_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & b_0 & b_1 & & \dots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ \vdots \\ a \end{matrix}}\right\} m \ \mathit{rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ \vdots \\ a \end{matrix}}\right\} n \ \mathit{rows} \end{matrix}$$

of order $m + n$.

Now we are ready to generalize Proposition 4 in the next theorem.

Theorem 4. *Let $\{\theta_0, \theta_1, \dots, \theta_{n-1}\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We assume that $Tr_n(\theta_0) \neq 0$ without loss of generality. Let $\varphi(x) = a_0x + a_1x^q \cdots + a_{n-1}x^{q^{n-1}}$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$ satisfying the resultant*

$$Res(a_0 + a_1t + \cdots + a_{n-1}t^{n-1}, 1 + t + \cdots + t^{n-1}) \neq 0. \tag{5}$$

Let $g_0, g_1 \dots, g_{n-1} \in \mathbb{F}_q[x]$ be such that $g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$ is an $(a_0 + \cdots + a_{n-1})$-permutation of $\mathbb{F}_q$. Then

$$F(x) = \varphi(x) + \theta_0 g_0(Tr_n(x)) + \cdots + \theta_{n-1} g_{n-1}(Tr_n(x))$$

is a permutation over $\mathbb{F}_{q^n}$.

Proof. We use a similar method as in the proof of Proposition 4. Take $g(x)$ of the form

$$g(x) = g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$$

and $h(x)$ as the constant function equal to 1. Let

$$\varphi(x) = a_0x + a_1x^q \cdots + a_{n-1}x^{q^{n-1}} \in \mathbb{F}_q[x]$$

with $a_0, \dots, a_{n-1}$ satisfying (5). For $x \in \mathbb{F}_q$ we have

$$\varphi(x) + Tr_n(g(x)) = (a_0 + \cdots + a_{n-1})x + g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1}).$$

This is a permutation polynomial over $\mathbb{F}_q$ since

$$g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$$

is an $(a_0 + \cdots + a_{n-1})$-permutation of $\mathbb{F}_q$. So condition 2 of [1, Proposition 5.6] holds.

The proof of $\ker \varphi \cap \ker Tr_n = \{0\}$ comes from an important property of the resultant [13, page 36] (see also, [12, Corollary 8.4, page 203]). It indicates that the polynomials $1 + t + \cdots + t^{n-1}$ and $a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ do not have common root if and only if (5) holds. Note that we also use q-associates before this argument. □

6 A Further Generalization of Linear Translators

For an arbitrary $\mathbb{F}_q$ and a map $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ with $n \geq 2$, the concept of linear structure in Definition 2 corresponds to the notion of linear structure: Let $\gamma \in \mathbb{F}_{q^n}$, $b \in \mathbb{F}_q$. Then γ is called b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ if

$$f(x + \gamma u) = f(x) + bu \text{ for all } x \in \mathbb{F}_{q^n} \text{ and } y \in \mathbb{F}_q.$$

Note that if $q = 2$, then b is either 0 or 1 and we have either 0-linear translator or 1-linear translator coinciding with 0-linear structure or 1-linear structure.

Recently Cepak, Pasalic and Muratović-Ribić generalized the notion of linear translators and gave an application for constructing permutation polynomials (see [8]).

In this section we obtain a further and very natural generalization of the notion of linear translators. We also give two different applications of our more general version to permutation polynomials. Theorem 5 is an easy but rather unexpected application. It gives a class of permutation polynomials over $\mathbb{F}_{q^n}$ using a surjective map $f : \mathbb{F}_{q^n} \to S \subseteq \mathbb{F}_q$ and our notion of generalized linear translator.

The proof uses a trick that was used earlier in [15]. Moreover, this method gives the inverse permutation explicitly.

The second application is Theorem 6 below and it shows that under certain conditions one can get permutation polynomials on $\mathbb{F}_{q^n}$ again using $f : \mathbb{F}_{q^n} \to S \subseteq \mathbb{F}_q$ and the corresponding generalized linear translator. Finally, we give an explicit example illustrating that there exist generalized linear translators satisfying the conditions of Theorem 6 and not being Frobenius linear translators, which is the notion expressed in [8].

We start with our generalization of the notion.

Definition 8. *Let $S \subseteq \mathbb{F}_q$ and let $\gamma, b \in \mathbb{F}_{q^n}$. Let $A : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an additive map. We say that γ is a (b, A)-linear translator with respect to S for the mapping $f : \mathbb{F}_{q^n} \to S$, if*

$$f(x + \gamma u) = f(x) + bA(u)$$

for all $x \in \mathbb{F}_{q^n}$ and for all $u \in S$.

Now we are ready to present a first application of the notion in Definition 8.

Theorem 5. *Let $S \subseteq \mathbb{F}_{q^n}$ and $f : \mathbb{F}_{q^n} \rightarrow S$ be a surjective map. Let $\gamma \in \mathbb{F}_q$ be a (b, A)-linear translator with respect to S for the map f where A is an additive map and $\gamma, b \in \mathbb{F}_{q^n}$. Then for any $g \in \mathbb{F}_{q^n}[x]$ which maps S into S, we have that $F(x) = x + \gamma g(f(x))$ is a permutation over $\mathbb{F}_{q^n}$ if and only if $\psi(z) = z + bA(g(z))$ is a permutation on S.*

Moreover, if F is a permutation over $\mathbb{F}_{q^n}$, then its inverse function F^{-1} is given explicitly as

$$F^{-1}(z) = z - \gamma g(\psi^{-1}(f(z))).$$

Proof. Let x be any element of $\mathbb{F}_{q^n}$. Then we have $F(x) = x + \gamma g(f(x))$ by definition. By applying f to the both sides of the equality we obtain

$$\begin{aligned} f(F(x)) &= f(x + \gamma g(f(x))) \\ &= f(x) + bA(g(f(x))) \text{ since } f \text{ is } (b, A) \text{-linear translator} \\ &= \psi(f(x)) \text{ by definition of the map } \psi. \end{aligned} \tag{6}$$

Therefore we have $\psi(f(x)) = f(F(x))$.

Assume first that ψ is a permutation over S. Let $F(x_1) = F(x_2)$ for some x_1,$x_2 \in \mathbb{F}_{q^n}$. Then applying f to both sides of the equality we have $f(F(x_1)) = f(F(x_2))$. By using (6), we obtain

$$\psi(f(x_1)) = f(F(x_1)) = f(F(x_2)) = \psi(f(x_2)).$$

Since ψ is a permutation over S, we get $f(x_1) = f(x_2)$. As $F(x_1) = F(x_2)$ we also have

$$x_1 + \gamma g(f(x_1)) = x_2 + \gamma g(f(x_2)).$$

These imply that $x_1 = x_2$. Therefore F is injective and indeed F is bijective.

Conversely, assume that F is a permutation over $\mathbb{F}_{q^n}$. Let s be any element of S. Since f is a surjective map, there exists $\alpha \in \mathbb{F}_{q^n}$ satisfying $f(\alpha) = s$. Because F is permutation over $\mathbb{F}_{q^n}$, there is $x \in \mathbb{F}_{q^n}$ such that $F(x) = \alpha$. By using (6), we have

$$\psi(f(x)) = f(F(x)) = f(\alpha) = s.$$

Therefore ψ is surjective and in fact, ψ is bijective. Then $F(x) = x + \gamma g(f(x))$ is a permutation over $\mathbb{F}_{q^n}$ if and only if $\psi(z) = z + bA(g(z))$ is a permutation over S.

Next, we compute F^{-1} explicitly. Let $y = F(x) = x + \gamma g(f(x))$. Then we have

$$\begin{aligned} f(y) &= f(x + \gamma g(f(x))) \\ &= f(x + \gamma u), \text{ where } u = g(f(x)) \in S \\ &= f(x) + bA(u), \text{ since } \gamma \text{ is a } (b, A)\text{-linear translator} \\ &= f(x) + bA(g(f(x))), \text{ recall } u = g(f(x)) \\ &= z + bA(g(z)), \text{ where } f(x) = z \\ &= \psi(z). \end{aligned}$$

As ψ is a permutation on S we have that for each y there exists $x = y - \gamma g(\psi^{-1}(f(y)))$ satisfying $F(x) = y$. Therefore, $F(x)$ is surjective and the desired result follows. The converse of the statement is proved similarly.

Moreover, $F^{-1}(z) = z - \gamma g(\psi^{-1}(f(z)))$ since $f^{-1}(z) = x$. □

Next, we give another application of Definition 8.

Theorem 6. *Let f be a function from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$, $\gamma \in \mathbb{F}_{q^n}^*$. Let γ be a (b, A)-linear translator of f where $b \in \mathbb{F}_q$ and $A(x) \in \mathbb{F}_{q^n}[x]$ is an additive map satisfying the following conditions:*

1. *A is $\mathbb{F}_q$-linear.*
2. *$A(\gamma) \neq 0$.*
3. *$A(\gamma a) = A(\gamma)A(a)$ for all $a \in \mathbb{F}_q$.*
4. *For any $x \in \mathbb{F}_{q^n}$: If $A(\gamma x) \in A(\gamma)\mathbb{F}_q$, then $x \in \mathbb{F}_q$.*
5. *$A|_{\mathbb{F}_q}$ is onto.*

For any map $h : \mathbb{F}_q \to \mathbb{F}_q$ consider the map

$$\begin{aligned} G : \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ x &\mapsto A(x) + A(\gamma)h(f(x)). \end{aligned}$$

Then G is a permutation over $\mathbb{F}_{q^n}$ if and only if the following derived map depending on h and b

$$\begin{aligned} g : \mathbb{F}_q &\to \mathbb{F}_q \\ u &\mapsto u + bh(u) \end{aligned}$$

is a permutation over $\mathbb{F}_q$.

Proof. We use a method similar to the ones in [11] or [8]. Let $x, \alpha \in \mathbb{F}_{q^n}$ satisfy $G(x) = G(x + \gamma\alpha)$. Then

$$\begin{aligned} G(x) &= A(x) + A(\gamma)h(f(x)), \\ G(x + \gamma\alpha) &= A(x + \gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)) \\ &= A(x) + A(\gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)) \text{ by condition 1,} \end{aligned}$$

and hence

$$A(\gamma)h(f(x)) = A(\gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)). \tag{7}$$

Divide both sides of Eq. (7) by $A(\gamma)$, since $A(\gamma) \neq 0$ by condition 2. Then we have

$$h(f(x)) = \frac{A(\gamma\alpha)}{A(\gamma)} + h(f(x + \gamma\alpha)).$$

As $f(x), f(x + \gamma\alpha) \in \mathbb{F}_q[x]$, $h \in \mathbb{F}_q[x]$ and $\frac{A(\gamma\alpha)}{A(\gamma)} \in \mathbb{F}_q$, by condition 4 we get $\alpha \in \mathbb{F}_q$. Taking $a = \alpha \in \mathbb{F}_q$, we have

$$h(f(x)) = \frac{A(\gamma a)}{A(\gamma)} + h(f(x + \gamma a)).$$

Note that $A(\gamma a) = A(\gamma)A(a)$ by condition 3, so we get

$$h(f(x)) = A(a) + h(f(x + \gamma a))$$

and hence by using that γ is a (b, A)-linear translator for f, we get

$$h(f(x)) = A(a) + h(f(x) + bA(a)).$$

Then substituting $u = f(x) \in \mathbb{F}_q[x]$, we have

$$h(u) = A(a) + h(u + bA(a)). \tag{8}$$

Consider

$$\begin{aligned} g(u) &= u + bh(u) \\ g(u + bA(a)) &= u + bA(a) + b(h(u + bA(a))) \\ &= u + b\,(A(a) + h(u + bA(a)) \\ &= u + bh(u) \\ &= g(u). \end{aligned}$$

Here as x runs through $\mathbb{F}_{q^n}$, $u = f(x)$ runs through $\mathbb{F}_q$ as f is onto. Then we get

$$g(u) = g(u + bA(a)). \tag{9}$$

Thus the mapping G is a permutation over $\mathbb{F}_{q^n}$ if and only if the only a satisfying Eq. (9) is $a = 0$. If $b = 0$, then we obtain that $A(a) = 0$ as g is permutation. As $A|_{\mathbb{F}_q}$ is one-to-one, we get $a = 0$. If $b = 0$, then from Eq. (8) we have

$$h(u) = A(a) + h(u + bA(a)) = A(a) + h(u).$$

Hence $A(a) = 0$. Therefore, $a = 0$. □

The next example illustrates a simple situation when the conditions of Theorem 6 hold. Note that the polynomial $A(x)$ in the next example is not in the form of a Frobenius linear translator. Moreover, the next example illustrates that the conditions of Theorem 5 hold easily as its conditions are weaker.

Example 2. Let $q = 2$ and $n = 4$. Take $A(x) = \alpha^2 x + \alpha^7 x^2 + \alpha^3 x^4 + \alpha^5 x^8 \in \mathbb{F}_{2^4}[x]$ where $\alpha^4 = 1 + \alpha$ and $\gamma = \alpha^3 \in \mathbb{F}_{2^4}^*$. Then $A(x)$ satisfies the following conditions:

1. A is $\mathbb{F}_2$-linear since A is additive.
2. $A(\gamma) \neq 0$ since $A(\gamma) = A(\alpha^3) = \alpha^4 \neq 0$.
3. $A(\gamma a) = A(\gamma)A(a)$ for all $a \in \mathbb{F}_2$ since

$$A(a) = \alpha^2 a + \alpha^7 a^2 + \alpha^3 a^4 + \alpha^5 a^8 = a(\alpha^2 + \alpha^7 + \alpha^3 + \alpha^5) = a$$

and

$$A(\gamma a) = \alpha^2(\alpha^3 a) + \alpha^7(\alpha^3 a)^2 + \alpha^3(\alpha^3 a)^4 + \alpha^5(\alpha^3 a)^8 = aA(\gamma) = A(a)A(\gamma).$$

4. For any $x \in \mathbb{F}_{q^n}$: If $A(\gamma x) \in A(\gamma)\mathbb{F}_q$, then $x \in \mathbb{F}_q$. Consider $\theta = \alpha^i \in \mathbb{F}_{2^4}/\mathbb{F}_2$ for $1 \leq i \leq 14$, then we have

$$A(\gamma\theta) = A(\gamma\alpha^i) \notin A(\gamma)\mathbb{F}_2 \text{ where } A(\gamma) = \alpha^4 \text{ for } 1 \leq i \leq 14.$$

Indeed, we have $\{A(\gamma\alpha^i) : 1 \leq i \leq 14\} = \mathbb{F}_{16} \setminus \{0, \alpha^4\}$. For example, $A(\gamma\alpha) = \alpha^8$ and $A(\gamma\alpha^{11}) = \alpha$.

5. $A|_{\mathbb{F}_2}$ is onto.

Let $f : \mathbb{F}_{2^4} \rightarrow \mathbb{F}_2$ be the map $x \mapsto Tr_4(x)$. Then α^3 is a $(1, A)$-linear translator of f since we have

$$\begin{aligned} f(x+\gamma u) = f(x+\alpha^3 u) &= Tr_4(x+\alpha^3 u) = Tr_4(x) + uTr_4(\alpha^3) \\ &= Tr_4(x) + u = f(x) + u \end{aligned}$$

for all $x \in \mathbb{F}_{2^4}$ and for all $u \in \mathbb{F}_2$.

7 Conclusion

We define a new class of Boolean functions which includes Cusick's class of functions [9] as a small subclass. We obtain explicit permutation polynomial classes over $\mathbb{F}_{q^2}$ via $\mathbb{F}_q$ and also over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 3$. We give a natural generalization of the notion of linear translators which is called (b,A)-linear translator. By using the connection between linear translators and permutation polynomials over finite fields, we obtain a class of permutation polynomials over $\mathbb{F}_{q^n}$. For applications our class of Boolean functions would be preferable compared to Cusick's class of functions mentioned above as our class is much larger having cryptographic properties as good as (or even better than) the class of Cusick's functions. Using our methods and new notion of (b,A)-linear translator it would be possible to construct further interesting algebraic structures like permutation polynomials or special functions.

Acknowledgments. We thank the reviewers for their insightful and fruitful remarks which greatly improved the presentation of the paper.

The research of the second and third authors has been funded by METU Coordinatorship of Scientific Research Projects via grant for projects GAP-101-2018-2782.

References

1. Akbary, A., Ghioca, D., Wang, Q.: On constructing permutations of finite fields. Finite Fields Appl. **17**(1), 51–67 (2011)
2. Boztaş, S., Özbudak, F., Tekin, E.: Explicit full correlation distribution of sequence families using plateaued functions. IEEE Trans. Inf. Theory **64**(4), 2858–2875 (2018)

3. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
4. Carlet, C.: On the properties of vectorial functions with plateaued components and their consequences on APN functions. In: El Hajji, S., Nitaj, A., Carlet, C., Souidi, E.M. (eds.) C2SI 2015. LNCS, vol. 9084, pp. 63–73. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-18681-8_5
5. Carlet, C.: Boolean and vectorial plateaued functions and APN functions. IEEE Trans. Inf. Theory **61**(11), 6272–6289 (2015)
6. Carlet, C., Mesnager, S., Özbudak, F., Sınak, A.: Explicit characterizations for plateaued-ness of *p*-ary (Vectorial) functions. In: El Hajji, S., Nitaj, A., Souidi, E.M. (eds.) C2SI 2017. LNCS, vol. 10194, pp. 328–345. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-55589-8_22
7. Cepak, N., Charpin, P., Pasalic, E.: Permutations via linear translators. Finite Fields Appl. **45**, 19–42 (2017)
8. Cepak, N., Pasalic, E., Muratović-Ribić, A.: Frobenius linear translators giving rise to new infinite classes of permutations and bent functions. arXiv preprint https://arxiv.org/abs/1801.08460 (2018)
9. Cusick, T.W.: Highly nonlinear plateaued functions. IET Inf. Secur. **11**(2), 78–81 (2017)
10. Cusick, T.W., Stănica, P.: Cryptographic Boolean Functions and Applications, 2nd edn. Academic Press, San Diego (2017). (1st ed., 2009)
11. Kyureghyan, G.M.: Constructing permutations of finite fields via linear translators. J. Comb. Theory Ser. A **118**, 1052–1061 (2011)
12. Lang, S.: Algebra. Graduate Texts in Mathematics, p. 211. Springer-Verlag, New York (2002)
13. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1983)
14. Mesnager, S.: Bent Functions: Fundamentals and Results. Springer, Cham (2016)
15. Mesnager, S., Ongan, P., Özbudak, F.: New bent functions from permutations and linear translators. In: El Hajji, S., Nitaj, A., Souidi, E.M. (eds.) C2SI 2017. LNCS, vol. 10194, pp. 282–297. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-55589-8_19
16. Mesnager, S., Özbudak, F., Snak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Des. Codes Crypt. **87**(2–3), 463–480 (2018). https://doi.org/10.1007/s10623-018-0556-4
17. Riera, C., Solé, P., Stănică, P.: A complete characterization of plateaued boolean functions in terms of their cayley graphs. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 2018. LNCS, vol. 10831, pp. 3–10. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-89339-6_1
18. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016)
19. Tokareva, N.: Bent Functions: Results and Applications to Cryptography. Academic Press, San Diego (2015)