On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$

Pascale Charpin[1] and Gohar M. Kyureghyan[2]

[1] INRIA, SECRET research Team, B.P. 105, 78153 Le Chesnay Cedex, France
pascale.charpin@inria.fr
[2] Department of Mathematics, Otto-von-Guericke-University Magdeburg,
Universitätsplatz 2, 39106 Magdeburg, Germany
gohar.kyureghyan@ovgu.de

Abstract. We study permutation polynomials of the shape $F(X) = G(X) + \gamma\, Tr(H(X))$ over $\mathbb{F}_{2^n}$. We prove that if the polynomial $G(X)$ is a permutation polynomial or a linearized polynomial, then the considered problem can be reduced to finding Boolean functions with linear structures. Using this observation we describe six classes of such permutation polynomials.

Keywords: Permutation polynomial, linear structure, linearized polynomial, trace, Boolean function.

1 Introduction

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A polynomial $F(X) \in \mathbb{F}_{2^n}[X]$ is called a permutation polynomial (PP) of $\mathbb{F}_{2^n}$ if the associated polynomial mapping

$$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto F(x)$$

is a permutation of $\mathbb{F}_{2^n}$. There are several criteria ensuring that a given polynomial is a PP, but those conditions are, however, rather complicated, cf. [7]. PP are involved in many applications of finite fields, especiallly in cryptography, coding theory and combinatorial design theory. Finding PP of a special type is of great interest for the both theoretical and applied aspects.

In this paper we study PP of the following shape

$$F(X) = G(X) + \gamma\, Tr(H(X)), \tag{1}$$

where $G(X), H(X) \in \mathbb{F}_{2^n}[X]$, $\gamma \in \mathbb{F}_{2^n}$ and $Tr(X) = \sum_{i=0}^{n-1} X^{2^i}$ is the polynomial defining the absolute trace function of $\mathbb{F}_{2^n}$. Examples of such polynomials are obtained in [3],[6] and [9]. We show that in the case the polynomial $G(X)$ is a PP or a linearized polynomial the considered problem can be reduced to finding Boolean functions with linear structures. We use this observation to describe six classes of PP of type (1).

S.W. Golomb et al. (Eds.): SETA 2008, LNCS 5203, pp. 368–376, 2008.

2 A Linear Structure of a Boolean Function

A Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be represented as $Tr(R(x))$ for some (not unique) mapping $R : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. A Boolean function $Tr(R(x))$ is said to have a linear structure $\alpha \in \mathbb{F}_{2^n}^*$ if

$$Tr(R(x)) + Tr(R(x + \alpha)) = Tr(R(x) + R(x + \alpha))$$

is a constant function. We call a linear structure c-linear structure if

$$Tr(R(x) + R(x + \alpha)) \equiv c,$$

where $c \in \mathbb{F}_2$. Given $\gamma \in \mathbb{F}_{2^n}^*$ and $c \in \mathbb{F}_2$, let $H_\gamma(c)$ denote the affine hyperplane defined by the equation $Tr(\gamma x) = c$, i.e.,

$$H_\gamma(c) = \{x \in \mathbb{F}_{2^n} \mid Tr(\gamma x) = c\}.$$

Then $\alpha \in \mathbb{F}_{2^n}^*$ is a c-linear structure for $Tr(R(x))$ if and only if the image set of the mapping $R(x) + R(x + \alpha)$ is contained in the affine hyperplane $H_1(c)$.

The Walsh transform of a Boolean function $Tr(R(x))$ is defined as follows

$$\mathcal{W} : \mathbb{F}_{2^n} \to \mathbb{Z},\ \lambda \mapsto \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(R(x)+\lambda x)}.$$

Whether a Boolean function $Tr(R(x))$ has a linear structure can be recognized from its Walsh transform.

Proposition 1 ([2,8]). *Let $c \in \mathbb{F}_2$ and $R : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. An element $\alpha \in \mathbb{F}_{2^n}^*$ is a $(c + 1)$-linear structure for $Tr(R(x))$ if and only if*

$$\mathcal{W}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(R(x)+\lambda x)} = 0$$

for all $\lambda \in H_\alpha(c)$.

In [5] all Boolean functions assuming a linear structure are characterized as follows.

Theorem 1 ([5]). *Let $R : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then the Boolean function $Tr(R(x))$ has a linear structure if and only if there is a non-bijective linear mapping $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that*

$$Tr(R(x)) = Tr\big(H \circ L(x) + \beta x\big) + c,$$

where $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $\beta \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$.

Clearly, any element from the kernel of L is a linear structure of $Tr(R(x))$ considered in Theorem 1. Moreover, those are the only ones if the mapping $Tr(H(x))$ has no linear structure belonging to the image of L. We record this observation in the following lemma to refer it later.

Lemma 1. *Let* $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be an arbitrary mapping. Then* $\gamma \in \mathbb{F}_{2^n}^*$ *is a linear structure of*

$$Tr\big(H(x^2 + \gamma x) + \beta x\big)$$

for any $\beta \in \mathbb{F}_{2^n}$*.*

Next lemma describes another family of Boolean functions having a linear structure. Its proof is straightforward.

Lemma 2. *Let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and* $\alpha \in \mathbb{F}_{2^n}^*$*. Then* α *is a linear structure of* $Tr(F(x) + F(x+\alpha) + \beta x)$ *for any* $\beta \in \mathbb{F}_{2^n}$*.*

In general, for a given Boolean function it is difficult to recognize whether it admits a linear structure. Slightly extending results from [4], we characterize all monomial Boolean functions assuming a linear structure. More precisely, for a given nonzero $a \in \mathbb{F}_{2^n}$, we describe all exponents s and nonzero $\delta \in \mathbb{F}_{2^n}$ such that a is a linear structure for the Boolean function $Tr(\delta x^s)$.

Let $0 \le s \le 2^n - 2$. We denote by C_s the cyclotomic coset modulo $2^n - 1$ containing s:

$$C_s = \{s, 2s, \ldots, 2^{n-1}s\} \pmod{2^n - 1}.$$

Note that if $|C_s| = l$, then $\{x^s \mid x \in \mathbb{F}_{2^n}\} \subseteq \mathbb{F}_{2^l}$ and $\mathbb{F}_{2^l}$ is the smallest such subfield.

The next lemma is an extension of Lemma 2 from [4].

Lemma 3. *Let* $0 \le s \le 2^n - 2$, $\delta \in \mathbb{F}_{2^n}^*$ *be such that the Boolean function* $Tr(\delta x^s)$ *is a nonzero function. Then* $a \in \mathbb{F}_{2^n}^*$ *is a linear structure of the Boolean function* $Tr(\delta x^s)$ *if and only if*

(a) $s = 2^i$ *and* a *is arbitrary*
(b) $s = 2^i + 2^j$ $(i \ne j)$ *and* $(\delta a^{2^i+2^j})^{2^{n-i}} + (\delta a^{2^i+2^j})^{2^{n-j}} = 0$*.*

Proof. Let $a \in \mathbb{F}_{2^n}^*$ be a linear structure for $Tr(\delta x^s)$. Then

$$Tr(\delta(x^s + (x+a)^s)) \equiv c \qquad (2)$$

holds for all $x \in \mathbb{F}_{2^n}$ and a fixed $c \in \mathbb{F}_2$. In [4] it is shown that in the case $|C_s| = n$ the identity (2) can be satisfied only if the binary weight of s does not exceed 2. On the other side it is easy to see that for an s of binary weight 1 the corresponding Boolean function $Tr(\delta x^s)$ is linear and thus any nonzero element is a linear structure. If $s = 2^i + 2^j$, then

$$\begin{aligned}
Tr(\delta(x^{2^i+2^j} + (x+a)^{2^i+2^j})) &= Tr\left(\delta a^{2^i+2^j}\left(\left(\frac{x}{a}\right)^{2^i} + \left(\frac{x}{a}\right)^{2^j}\right)\right) + Tr\left(\delta a^{2^i+2^j}\right) \\
&= Tr\left(\left((\delta a^{2^i+2^j})^{2^{n-i}} + (\delta a^{2^i+2^j})^{2^{n-j}}\right)\frac{x}{a}\right) \\
&\quad + \ Tr\left(\delta a^{2^i+2^j}\right),
\end{aligned}$$

implying (b). To complete the proof, we need to consider the case $|C_s| = l < n$. Let $n = lm$. Then

$$Tr(\delta(x^s + (x+a)^s)) = Tr(\beta(y^s + (y+1)^s)),$$

where $y = x/a$ and $\beta = \delta a^s$. We write $i \prec s$ if $i \neq s$ and the binary representation of i is covered by the one of s. Then

$$Tr(\beta(y^s + (y+1)^s)) = \sum_{i \prec s} Tr(\beta y^i) = \sum_{k \prec s,\ k \text{ is a coset repr.}} Tr(\beta_k y^k).$$

Note that the exponents in the monomial summands $Tr(\beta_k y^k)$ are from different cyclotomy cosets. Hence to have

$$\sum_{k \prec s,\ k \text{ is a coset repr.}} Tr(\beta_k y^k) \equiv c$$

it is necessary that $c = Tr(\beta)$ and $Tr(\beta_k y^k) \equiv 0$ for all $k \neq 0$. Consider $k_0 \prec s$ such that $k_0 = s - 2^i$. Lemma 3 of [1] implies that $|C_{k_0}| = n$, and therefore $Tr(\beta_{k_0} y^{k_0}) \equiv 0$ holds only if $\beta_{k_0} = 0$. Further $\beta_{k_0} = \beta + \beta^{2^l} + \ldots \beta^{2^{l(m-1)}} = Tr_l^n(\beta)$, where Tr_v^u denotes the trace function from $\mathbb{F}_{2^u}$ onto its subfield $\mathbb{F}_{2^v}$. Hence necessarily $Tr_l^n(\beta) = Tr_l^n(\delta a^s) = a^s Tr_l^n(\delta) = 0$, and thus the Boolean function

$$Tr\left(\delta x^s\right) = Tr_1^l\left(x^s Tr_l^n(\delta)\right)$$

is the zero function. □

Observe that $\delta = a^{-(2^i+2^j)}$ satisfies condition (b) of Lemma 3.

3 Permutation Polynomials

In this section we study permutation polynomials of the shape

$$F(X) = G(X) + \gamma Tr(H(X)),$$

where $G(X), H(X) \in \mathbb{F}_{2^n}[X],\ \gamma \in \mathbb{F}_{2^n}$. Firstly we observe the following necessary property of $G(X)$.

Claim. Let $G(X), H(X) \in \mathbb{F}_{2^n}[X]$ and $\gamma \in \mathbb{F}_{2^n}$. If

$$F(X) = G(X) + \gamma Tr(H(X))$$

is a PP of $\mathbb{F}_{2^n}$, then for any $\beta \in \mathbb{F}_{2^n}$ there are at most 2 elements $x_1, x_2 \in \mathbb{F}_{2^n}$ such that $G(x_1) = G(x_2) = \beta$.

Proof. Suppose there are different x_1, x_2, x_3 with $G(x_1) = G(x_2) = G(x_3) = \beta$. Then F cannot be a PP, since $F(x_i) \in \{\beta, \beta + \gamma\}$ for $i = 1, 2, 3$. □

Proposition 2. *Let $G(X), H(X) \in \mathbb{F}_{2^n}[X]$ and $\gamma \in \mathbb{F}_{2^n}$. Then*

$$F(X) = G(X) + \gamma Tr(H(X))$$

is a PP of $\mathbb{F}_{2^n}$ if and only if for any $\lambda \in \mathbb{F}_{2^n}^*$ it holds

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x))} = 0 \quad \text{if } Tr(\gamma\lambda) = 0 \tag{3}$$

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x) + H(x))} = 0 \quad \text{if } Tr(\gamma\lambda) = 1. \tag{4}$$

Proof. Recall that $F(X)$ is a PP if and only if

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x))} = 0$$

for all $\lambda \in \mathbb{F}_{2^n}^*$, cf. [7]. Since

$$Tr(\lambda F(x)) = Tr(\lambda G(x)) + Tr(H(x))Tr(\gamma\lambda) = Tr(\lambda G(x) + H(x)Tr(\gamma\lambda)),$$

it must hold

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x))} = \begin{cases} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x))} = 0 & \text{if } Tr(\gamma\lambda) = 0 \\ \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x) + H(x))} = 0 & \text{if } Tr(\gamma\lambda) = 1. \end{cases}$$

□

Next we consider polynomials $F(X) = G(X) + \gamma Tr(H(X))$, where $G(X)$ is a PP or a linearized polynomial.

3.1 $G(X)$ Is a Permutation Polynomial

Firstly we establish a connection of the considered problem with the Boolean functions assuming a linear structure.

Theorem 2. *Let $G(X), H(X) \in \mathbb{F}_{2^n}[X]$, $\gamma \in \mathbb{F}_{2^n}$ and $G(X)$ be a PP. Then*

$$F(X) = G(X) + \gamma Tr(H(X)) \tag{5}$$

is a PP of $\mathbb{F}_{2^n}$ if and only if $H(X) = R(G(X))$, where $R(X) \in \mathbb{F}_{2^n}[X]$ and γ is a 0-linear structure of the Boolean function $Tr(R(x))$.

Proof. Since $G(X)$ is a PP, condition (3) is satisfied. Let G^{-1} be the inverse mapping of the associated mapping of G. Then condition (4) is equivalent to

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x) + H(x))} = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda y + H(G^{-1}(y)))} = 0$$

for all $\lambda \in \mathbb{F}_{2^n}$ with $Tr(\gamma\lambda) = 1$. Proposition 1 completes the proof. □

From Theorem 2 it follows that any PP of type (5) is obtained by substituting $G(X)$ into a PP of shape $X + \gamma Tr(R(X))$. The next theorem describes two classes of such polynomials.

Theorem 3. *Let $\gamma, \beta \in \mathbb{F}_{2^n}$ and $H(X) \in \mathbb{F}_{2^n}[X]$.*

(a) *Then the polynomial*

$$X + \gamma\, Tr\left(H(X^2 + \gamma X) + \beta X\right)$$

is PP if and only if $Tr(\beta\gamma) = 0$.

(b) *Then the polynomial*

$$X + \gamma\, Tr\left(H(X) + H(X+\gamma) + \beta X\right)$$

is PP if and only if $Tr(\beta\gamma) = 0$.

Proof. (a) By Theorem 2 the considered polynomial is a PP if and only if γ is a 0-linear structure of $Tr\left(H(x^2+\gamma x) + \beta x\right)$. To complete the proof note that

$$Tr\left(H((x+\gamma)^2 + \gamma(x+\gamma)) + \beta(x+\gamma)\right) + Tr\left(H(x^2+\gamma x) + \beta x\right) = Tr(\beta\gamma).$$

(b) The proof follows from Lemma 2 and Theorem 2 similarly to the previous case. □

Our next goal is to characterize all permutation polynomials of shape $X + \gamma\, Tr(\delta X^s + \beta X)$. Firstly, observe that if $s = 2^i$, then Theorem 2 yields that $X + \gamma\, Tr(\delta X^{2^i} + \beta X)$ is a PP if and only if $Tr(\delta\gamma^{2^i} + \beta\gamma) = 0$. The remaining cases are covered in the following theorem.

Theorem 4. *Let $\gamma, \beta \in \mathbb{F}_{2^n}$ and $3 \le s \le 2^n - 2$ be of binary weight ≥ 2. Let $\delta \in \mathbb{F}_{2^n}$ be such that the Boolean function $x \mapsto Tr(\delta x^s),\ x \in \mathbb{F}_{2^n}$, is not the zero function. Then the polynomial*

$$X + \gamma\, Tr(\delta X^s + \beta X)$$

is PP if and only if $s = 2^i + 2^j,\ (\delta\gamma^{2^j})^{2^{n-i}} + (\delta\gamma^{2^i})^{2^{n-j}} = 0$ and $Tr(\delta\gamma^{2^i+2^j} + \beta\gamma) = 0$.

Proof. By Theorem 2 the polynomial $X + \gamma\, Tr(\delta X^s + \beta X)$ defines a permutation if and only if γ is a 0-linear structure of $Tr(\delta x^s + \beta x)$. Then Lemma 3 implies that the binary weight of s must be 2. Note that for $s = 2^i + 2^j$ it holds

$$\begin{aligned} & Tr(\delta(x+\gamma)^{2^i+2^j} + \beta(x+\gamma)) \ + \ Tr(\delta x^{2^i+2^j} + \beta x) \\ = \quad & Tr(\delta x^{2^i}\gamma^{2^j} + \delta x^{2^j}\gamma^{2^i} + \delta\gamma^{2^i+2^j} + \beta\gamma) \\ = & \ Tr\left(\left((\delta\gamma^{2^j})^{2^{n-i}} + (\delta\gamma^{2^i})^{2^{n-j}}\right)x\right) + Tr(\delta\gamma^{2^i+2^j} + \beta\gamma). \end{aligned}$$

Thus γ is a 0-linear structure of $Tr(\delta x^s + \beta x)$ if and only if $(\delta\gamma^{2^j})^{2^{n-i}} + (\delta\gamma^{2^i})^{2^{n-j}} = 0$ and $Tr(\delta\gamma^{2^i+2^j} + \beta\gamma) = 0$. □

As an application of Theorem 4 we get the complete characterization of PP of type $X^d + Tr(X^t)$.

Corollary 1. *Let $1 \le d, t \le 2^n - 2$. Then*

$$X^d + Tr(X^t)$$

is PP over $\mathbb{F}_{2^n}$ if and only if the following conditions are satisfied:

- *n is even*
- *$gcd(d, 2^n - 1) = 1$*
- *$t = d \cdot s \pmod{2^n - 1}$ for some s such that $1 \le s \le 2^n - 2$ and has binary weight 1 or 2.*

Proof. By Claim 3 the considered polynomial defines a permutation on $\mathbb{F}_{2^n}$ only if X^d does it, which forces $\gcd(d, 2^n - 1) = 1$. Let d^{-1} be the multiplicative inverse of d modulo $2^n - 1$. Then $X^d + Tr(X^t)$ is PP if and only if $X + Tr(X^{d^{-1} \cdot t})$ is PP. Theorems 2 and 4 with $\gamma = \delta = 1$ and $\beta = 0$ imply that the later polynomial is PP if and only if $d^{-1} \cdot t = 2^i + 2^j \pmod{2^n - 1}$ with $i \ge j$ and $Tr(1) = 0$. Finally note that $Tr(1) = 0$ if and only if n is even. □

3.2 $G(X)$ Is a Linearized Polynomial

Let $G(X) = L(X)$ be a linearized polynomial over $\mathbb{F}_{2^n}$. In this subsection we characterize elements $\gamma \in \mathbb{F}_{2^n}$ and polynomials $H(X) \in \mathbb{F}_{2^n}[X]$ for which $L(X) + \gamma Tr(H(X))$ is PP. By Claim 3 the mapping defined by L must necessarily be bijective or 2-to-1. Since the case of bijective L is covered in the previous subsection, we consider here 2-to-1 linear mappings.

Lemma 4. *Let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a linear 2-to-1 mapping with kernel $\{0, \alpha\}$ and $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. If for some $\gamma \in \mathbb{F}_{2^n}$ the mapping*

$$N(x) = L(x) + \gamma Tr(H(x))$$

is a permutation of $\mathbb{F}_{2^n}$, then γ does not belong to the image set of L. Moreover, for such an element γ the mapping $N(x)$ is a permutation if and only if α is a 1-linear structure for $Tr(H(x))$.

Proof. Note that if γ belongs to the image set of L, then the image set of N is contained in that of L. In particular, N is not a permutation. We suppose now γ does not belong to the image set of L. It holds

$$N(x) = \begin{cases} L(x) & \text{if } Tr(H(x)) = 0 \\ L(x) + \gamma & \text{if } Tr(H(x)) = 1, \end{cases}$$

and for all $x \in \mathbb{F}_{2^n}$ we have

$$N(x) + N(x + \alpha) = \gamma Tr(H(x) + H(x + \alpha)).$$

Thus, if N is a permutation, then $Tr(H(x) + H(x + \alpha)) = 1$ for all x, *i.e.*, α is a 1-linear structure for $Tr(H(x))$. Conversely, assume that

$$Tr(H(x) + H(x + \alpha)) = 1 \quad \text{for all} \quad x \in \mathbb{F}_{2^n}. \tag{6}$$

Let $y, z \in \mathbb{F}_{2^n}$ be such that $N(y) = N(z)$. If $Tr(H(y) + H(z)) = 0$ then

$$N(y) + N(z) = L(y + z) = 0,$$

and hence $y + z \in \{0, \alpha\}$. Further, (6) forces $y = z$. To complete the proof, observe that $Tr(H(y) + H(z)) = 1$ is impossible, since it implies

$$N(y) + N(z) = L(y + z) + \gamma = 0,$$

which contradicts the assumption that γ is not in the image set of L. □

Lemmas 1, 2 in combination with Lemma 4 imply the following classes of PP.

Theorem 5. *Let $L \in \mathbb{F}_{2^n}[X]$ be a linearized polynomial, defining a 2- to -1 mapping with kernel $\{0, \alpha\}$. Further let $H \in \mathbb{F}_{2^n}[X]$, $\beta \in \mathbb{F}_{2^n}$ and $\gamma \in \mathbb{F}_{2^n}$ be not in the image set of L.*

(a) *The polynomial*

$$L(X) + \gamma Tr\left(H(X^2 + \alpha X) + \beta X\right)$$

is PP if and only if $Tr(\beta\alpha) = 1$.

(b) *The polynomial*

$$L(X) + \gamma Tr\left(H(X) + H(X + \alpha) + \beta X\right)$$

is PP if and only if $Tr(\beta\alpha) = 1$.

Remark 1. To apply Theorem 5 we need to have a linearized 2- to -1 polynomial with known kernel and image set. An example of such a polynomial is $X^{2^k} + \alpha^{2^k - 1}X$ where $1 \le k \le n - 1$ with $\gcd(k, n) = 1$ and $\alpha \in \mathbb{F}_{2^n}^*$. The kernel of its associated mapping is $\{0, \alpha\}$ and the image set is $H_{\alpha^{-2^k}}(0)$. Moreover, any linear 2- to -1 mapping with kernel $\{0, \alpha\}$ (or image set $H_{\alpha^{-2^k}}(0)$) can be obtained as a left (or right) composition of this mapping with an appropriate bijective linear mapping.

The next result is a direct consequence of Lemmas 3 and 4.

Theorem 6. *Let $L \in \mathbb{F}_{2^n}[X]$ be a linearized polynomial defining a 2- to -1 mapping with kernel $\{0, \alpha\}$. Let $\beta, \gamma \in \mathbb{F}_{2^n}$ and γ do not belong to the image set of L. If $3 \le s \le 2^n - 2$ is of binary weight ≥ 2, then the polynomial*

$$L(X) + \gamma Tr(\delta X^s + \beta X)$$

is PP if and only if $s = 2^i + 2^j$, $(\delta\alpha^{2^j})^{2^{n-i}} + (\delta\alpha^{2^i})^{2^{n-j}} = 0$ and $Tr(\delta\alpha^{2^i + 2^j} + \beta\alpha) = 1$.

Theorem 6 yields the complete characterization of PP of type $X^{2^k}+X+Tr(X^s)$.

Corollary 2. *Let $1 \leq k \leq n-1$ and $1 \leq s \leq 2^n-2$. Then*

$$X^{2^k} + X + Tr(X^s)$$

is PP over $\mathbb{F}_{2^n}$ if and only if the following conditions are satisfied:

- *n is odd*
- *$gcd(k, n) = 1$*
- *s has binary weight 1 or 2.*

Proof. Firstly observe that the polynomial $X^{2^k}+X$ has at least two zeros, 0 and 1. Hence from Claim 3 it follows that if $X^{2^k}+X+Tr(X^s)$ is PP then necessarily the mapping $L(x) = x^{2^k} + x$ is 2-to-1. This holds if and only if $\gcd(k, n) = 1$. Further note that the image set of such an L is the hyperplane $H_1(0)$. Hence $\gamma = 1$ does not belong to the image set of L if and only if $Tr(1) = 1$, equivalently if n is odd. The rest of the proof follows from Lemma 4 and Theorem 6 with $\alpha = \delta = 1$ and $\beta = 0$. □

Remark 2. Some results of this paper are valid also in the finite fields of odd characteristic. In a forthcoming paper we will report more accurately on that.

References

1. Bierbrauer, J., Kyureghyan, G.: Crooked binomials. Des. Codes Cryptogr. 46, 269–301 (2008)
2. Dubuc, S.: Characterization of linear structures. Des. Codes Cryptogr. 22, 33–45 (2001)
3. Hollmann, H.D.L., Xing, Q.: A class of permutation polynomials of $\mathbb{F}_{2^n}$ related to Dickson polynomials. Finite Fields Appl. 11(1), 111–122 (2005)
4. Kyureghyan, G.: Crooked maps in $\mathbb{F}_{2^n}$. Finite Fields Appl. 13(3), 713–726 (2007)
5. Lai, X.: Additive and linear structures of cryptographic functions. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 75–85. Springer, Heidelberg (1995)
6. Laigle-Chapuy, Y.: A note on a class of quadratic permutations over F_{2^n}. In: Boztaş, S., Lu, H.-F(F.) (eds.) AAECC 2007. LNCS, vol. 4851, pp. 130–137. Springer, Heidelberg (2007)
7. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications 20
8. Yashchenko, V.V.: On the propagation criterion for Boolean functions and bent functions. Problems of Information Transmission 33(1), 62–71 (1997)
9. Yuan, J., Ding, C., Wang, H., Pieprzyk, J.: Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$. Finite Fields Appl. 14(2), 482–493 (2008)