Contemporary Mathematics
Volume **518**, 2010

# Monomial functions with linear structure and permutation polynomials

Pascale Charpin and Gohar M. Kyureghyan

ABSTRACT. We characterize the monomial functions $Tr(\delta x^d)$ from a finite field into its prime subfield having linear structure. Using this result and the methods introduced in [**6**], we construct permutation polynomials of finite fields with few non-zero terms.

## 1. Introduction

Let $p$ be a prime number, $\mathbb{F}_{p^n}$ be a finite field of order $p^n$ and $\mathbb{F}_p$ be its prime subfield. In this paper we use $F(x)$ to denote a mapping, while $F(X)$ is reserved for a polynomial. Also, we generally use the term "mapping" to refer $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, while we use "function" for a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ in order to emphasize that the image set of $f$ is contained in $\mathbb{F}_p$.

Any mapping of $\mathbb{F}_{p^n}$ into itself is given by a unique polynomial of degree less than $p^n$. A polynomial $F(X) \in \mathbb{F}_{p^n}[X]$ is called a *permutation polynomial* of $\mathbb{F}_{p^n}$ if the mapping $x \mapsto F(x)$ is a permutation of $\mathbb{F}_{p^n}$. The construction of infinite classes of permutation polynomials over finite fields is an interesting and widely open problem, which is of great importance for a variety of theoretical and practical applications. Polynomials consisting of few non-zero terms are called sparse. Obtaining sparse permutation polynomials is of a particular interest.

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $c \in \mathbb{F}_p$. We say that $\alpha \in \mathbb{F}_{p^n}^*$ is a $c$-linear structure of the function $f$ if

$$f(x+\alpha) - f(x) = c \quad \text{for all} \quad x \in \mathbb{F}_{p^n}.$$

The concept of a linear structure was introduced in cryptography, mainly for Boolean functions. Functions with linear structures are considered as weak for some cryptographic applications. For example, a recent attack on hash functions proposed in [**4**] exploits a similar weakness of the involved mappings. In [**6**] it is shown that functions with linear structures yield permutation polynomials of the shape

$$F(X) = G(X) + \gamma\, Tr\big(H(X)\big),\ \gamma \in \mathbb{F}_{p^n},\ G(X),\ H(X) \in \mathbb{F}_{p^n}[X], \tag{1}$$

2010 *Mathematics Subject Classification.* Primary: 12E20, 12E05; Secondary: 94A60.
*Key words and phrases.* Permutation polynomial, linear permutation, monomials, $p$-to-1 mapping, linear structure, linear space, Boolean function, APN function.

where $Tr(X)$ is the polynomial defining the absolute trace function of $\mathbb{F}_{p^n}$. Here we apply these methods to construct sparse permutation polynomials by choosing both $G(X)$ and $H(X)$ to be monomials.

This paper is organized as follows: Section 2 summarizes the properties of functions with linear structure. Our main result is Theorem 5, which describes the linear space of a monomial function $Tr(\delta x^d)$ from a finite field into its prime subfield. Using this result and methods introduced in [**5, 6**] we construct sparse permutation polynomials in Theorems 6 and 7. Section 4 studies the properties of mappings of the shape $X^s + \gamma Tr(X^t)$ relevant for cryptological applications.

**Notation:** We denote by $|E|$ the cardinality of a set $E$. The trace function from $\mathbb{F}_{p^n}$ to any subfield $\mathbb{F}_{p^k}$ of $\mathbb{F}_{p^n}$ will be denoted as follows:

$$Tr_{n/k}(y) = y + y^{p^k} + \cdots + y^{p^{k(n/k-1)}}.$$

The absolute trace function (*i.e.*, $k = 1$) is simply denoted by $Tr$.

## 2. Preliminary results

Every function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be represented by $Tr(R(x))$ for some (not unique) mapping $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. In this paper we will need the following basic facts on functions with linear structures; for more details see [**6**].

Definition 1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $c \in \mathbb{F}_p$. We say that $\alpha \in \mathbb{F}_{p^n}^*$ is a $c$-linear structure of the function $f$ if*

$$f(x+\alpha) - f(x) = c \quad \text{for all} \quad x \in \mathbb{F}_{p^n}. \tag{2}$$

Note that if $\alpha$ is a $c$-linear structure of $f$, then necessarily $c = f(\alpha) - f(0)$.

Proposition 1 ([**11**]). *Let $\alpha, \beta \in \mathbb{F}_{p^n}^*$, $\alpha + \beta \neq 0$ and $a, b \in \mathbb{F}_p$. If $\alpha$ is an $a$-linear structure and $\beta$ is a $b$-linear structure of a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ , then*

$$\alpha + \beta \text{ is an } (a+b) - \text{linear structure of } f$$

*and for any $c \in \mathbb{F}_p^*$*

$$c \cdot \alpha \text{ is a } (c \cdot a) - \text{linear structure of } f.$$

*In particular, if $\Lambda^*$ is the set of linear structures of $f$, then $\Lambda = \Lambda^* \cup \{0\}$ is an $\mathbb{F}_p$-linear subspace, which we call the* linear space *of $f$.*

The following theorem characterizes the functions with linear structures.

Theorem 1 ([**6, 11**]). *Let $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $f = Tr \circ R$. Then $f$ has a linear structure if and only if there is a non-bijective linear mapping $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that*

$$f(x) = Tr(R(x)) = Tr\big(H \circ L(x) + \beta x\big) \tag{3}$$

*for some $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\beta \in \mathbb{F}_{p^n}$. In this case, the linear space of $f$ contains the kernel of $L$.*

Lemma 1 is a direct consequence of Theorem 1. For a given non-zero element $\gamma \in \mathbb{F}_{p^n}$, it describes functions for which this $\gamma$ is a linear structure.

Lemma 1. *Let $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an arbitrary mapping, $\gamma, \beta \in \mathbb{F}_{p^n}$, $\gamma \neq 0$ and $c = Tr\big(\beta\gamma\big)$. Then $\gamma$ is a $c$-linear structure of $f(x) = Tr(R(x))$ where*

$$R(x) = H(x^p - \gamma^{p-1}x) + \beta x.$$

Lemma 1 shows that it is easy to construct a function such that a given element is a linear structure of it. However, the characterization of all polynomials $R(X) \in \mathbb{F}_{p^n}[X]$, such that the induced function $Tr(R(x))$ has a linear structure, is very difficult.

In [**5, 6, 10**] methods for constructing permutation polynomials of shape (1) using functions with linear structure are introduced. We recall some of these results which are used in this paper.

CLAIM 1 ([**6**]). *Let $F(X) \in \mathbb{F}_{p^n}[X]$ be a polynomial of type (1). Assume that $F(x)$ is a permutation. Then for any $\beta \in \mathbb{F}_{p^n}$ there are at most $p$ elements $x \in \mathbb{F}_{p^n}$ with $G(x) = \beta$.*

THEOREM 2 ([**6**]). *Let $G(x)$ be a permutation of $\mathbb{F}_{p^n}$ and $\gamma \in \mathbb{F}_{p^n}$ be a $b$-linear structure of $Tr(R(x))$. Then we have:*

**(i):** *$F(x) = G(x) + \gamma\, Tr(R(G(x)))$ is a permutation of $\mathbb{F}_{p^n}$ if $b \neq -1$.*
**(ii):** *$F(x) = G(x) + \gamma\, Tr(R(G(x)))$ is a $p$-to-1 mapping of $\mathbb{F}_{p^n}$ if $b = -1$.*

If $p = 2$, then statement (i) of Theorem 2 can be strengthen to:

THEOREM 3 ([**5**]). *Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a permutation of $\mathbb{F}_{2^n}$, $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and $\gamma \in \mathbb{F}_{2^n}^*$. Then the mapping $F(x) = G(x) + \gamma\, f(x)$ is a permutation on $\mathbb{F}_{2^n}$ if and only if $\gamma$ is a 0-linear structure of $f \circ G^{-1}$, where $G^{-1}$ denotes the inverse mapping of $G$.*

## 3. Monomial functions with a linear structure

In this section we characterize all monomial functions assuming a linear structure. To be more precise, we describe the integers $s$ and nonzero elements $\delta \in \mathbb{F}_{p^n}$ for which the function $Tr(\delta x^s)$ has a linear structure.

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

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

It is easy to see that if the cardinality $|C_s| = \ell$, then $\{x^s \mid x \in \mathbb{F}_{p^n}\} \subseteq \mathbb{F}_{p^\ell}$ and $\mathbb{F}_{p^\ell}$ is the smallest such subfield.

CLAIM 2. *A nonzero element $a \in \mathbb{F}_{p^n}$ is a linear structure of $Tr(\delta x^s)$ if and if (a) or (b) holds:*

(a) *$a$ is a linear structure of $Tr(\delta^{p^i} x^{sp^i})$*
(b) *1 is a linear structure of $Tr(\delta a^s x^s)$.*

PROOF. The statements follow from an easy observation:

$$\begin{aligned} Tr\left(\delta^{p^i}\left((x+a)^{sp^i} - x^{p^i s}\right)\right) &= Tr\left(\delta\left((x+a)^s - x^s\right)\right) \\ &= Tr\left(\delta a^s\left(\left(\frac{x}{a}+1\right)^s - \left(\frac{x}{a}\right)^s\right)\right). \end{aligned}$$

□

Let $(s_{n-1}\, s_{n-2} \ldots s_0)_p$ be the base $p$ representation of $s$, *i.e.*, $s = \sum_{i=0}^{n-1} s_i p^i$ where $0 \leq s_i \leq p-1$. We first introduce some definitions.

- The *$p$-ary weight of $s$* is the sum $\sum_{i=0}^{n-1} s_i \in \mathbb{Z}$.
- The ($p$-ary) *Hamming weight of $s$* is the number of nonzero digits in its base $p$ representation.

Note that these two concepts coincide if and only if $p = 2$.

- We say that $(s_{n-1}\, s_{n-2} \dots s_0)_p$ is the *i-th shift* of $(s'_{n-1}\, s'_{n-2} \dots s'_0)_p$ if $s_j = s'_{j+i}$ for every $j$, where indices are taken modulo $n$.
- For any $s = (s_{n-1} \dots s_0)_p$ and $t = (t_{n-1} \dots t_0)_p$ we write $t \prec s$ when $s$ strictly covers $t$, that is

$$t \prec s \iff t \neq s \text{ and } t_i \leq s_i \text{ for any } i. \tag{4}$$

Notation $\preceq$ is used when $t = s$ is allowed.

Observe, that the integers $s$ and $s'$ are in the same cyclotomic coset modulo $p^n - 1$ if and only if their base $p$ representation are shifts of each other. Moreover, $|C_s| < n$ if and only if the base $p$ representation of $s$ has period $|C_s| = \ell$ where $\ell$ divides $n$. The next result implies in particular that it is impossible to have $|C_s| < n$ and $|C_{s-1}| < n$ simultaneously. This fact will be used later.

PROPOSITION 2. *Let $1 \leq s, t \leq p^n - 2$ be such that $|C_s| < n$ and $|C_t| < n$. Then $\gcd(p^n - 1, s - t) \neq 1$.*

PROOF. Set $|C_s| = \ell$ and $|C_t| = m$. Since $m$ and $\ell$ are proper divisors of $n$ we have $1 \leq \ell, m \leq n/2$. Further

$$\{x^s \mid x \in \mathbb{F}_{p^n}\} \subseteq \mathbb{F}_{p^\ell} \text{ and } \{x^t \mid x \in \mathbb{F}_{p^n}\} \subseteq \mathbb{F}_{p^m}.$$

Hence for any $x \in \mathbb{F}_{p^n}$ we have $x^{s-t} = y \cdot z$ for some $y \in \mathbb{F}_{p^\ell}$ and $z \in \mathbb{F}_{p^m}$. If $gcd(p^n - 1, s - t) = 1$ then $x \mapsto x^{s-t}$ is a permutation on $\mathbb{F}_{p^n}$ implying

$$|\{y \cdot z \mid y \in \mathbb{F}_{p^\ell},\ z \in \mathbb{F}_{p^m}\}| = p^n. \tag{5}$$

But the above cardinality can be upper bounded as follows

$$|\{y \cdot z \mid y \in \mathbb{F}_{p^\ell},\ z \in \mathbb{F}_{p^m}\}| \leq 1 + (p^\ell - 1)(p^m - 1) < p^{\ell+m} \leq p^n,$$

which shows that (5) cannot hold, completing the proof. □

We use also the following well known facts.

THEOREM 4 (Lucas Theorem). *Let $d = (d_{n-1}\, d_{n-2} \dots d_0)_p$ and $m = (m_{n-1}\, m_{n-2} \dots m_0)_p$. Then*

$$\binom{d}{m} \equiv \binom{d_{n-1}}{m_{n-1}} \cdots \binom{d_0}{m_0} \pmod{p}.$$

*In particular, $\binom{d}{m} \equiv 0 \pmod{p}$ as soon as $d_i < m_i$ for at least one $i$, so that*

$$\binom{d}{m} \not\equiv 0 \pmod{p} \text{ if and only if } m \preceq d.$$

CLAIM 3. *Let $\delta \in \mathbb{F}_{p^n}$ and $1 \leq s \leq p^n - 2$.*

(a) *Let $|C_s| = n$. Then $Tr(\delta x^s)$ is constant on $\mathbb{F}_{p^n}$ if and only if $\delta = 0$.*
(b) *Let $|C_s| = \ell < n$. Then $Tr(\delta x^s)$ is constant on $\mathbb{F}_{p^n}$ if and only if*

$$Tr_{n/\ell}(\delta) = \delta + \delta^{p^\ell} + \cdots + \delta^{p^{(n/\ell-1)\ell}} = 0.$$

(c) *Let $1 \leq s_i \leq p^n - 2$, $i \in I$, be from different cyclotomic cosets and $Tr(\delta_i x^{s_i})$ be nonzero mappings. Then $\sum_{i \in I} \alpha_i Tr(\delta_i x^{s_i}), \alpha_i \in \mathbb{F}_{p^n}$, is constant on $\mathbb{F}_{p^n}$ if and only if $\alpha_i = 0$ for all $i \in I$.*

PROOF. (a) Suppose $\delta \neq 0$. Let $c \in \mathbb{F}_p$ and consider the polynomial

$$f(X) = \delta X^s + \cdots + (\delta X^s)^{p^{n-1}} + c,$$

which induces the function $x \mapsto Tr(\delta x^s) + c$ on $\mathbb{F}_{p^n}$. The same function is described by the unique polynomial $g(X) \equiv f(X) \pmod{X^{p^n} - X}$ of degree strictly less than $p^n$. Observe that $g(X) = \sum_{t \in C_s} \delta_t X^t \pmod{X^{p^n} - X}$ with $\delta_t \in \{\delta, \ldots, \delta^{p^{n-1}}\}$. In particular, $g(X)$ is not the zero polynomial and cannot have $p^n$ zeroes in $\mathbb{F}_{p^n}$.

(b) We set again $f(x) = Tr(\delta x^s) + c$ for some $c \in \mathbb{F}_p$. Since $x^s \in \mathbb{F}_{p^\ell}$ for any $x \in \mathbb{F}_{p^n}$, we have

$$f(x) = Tr_{\ell/1}\left(Tr_{n/\ell}(\delta)x^s\right) + c.$$

As above, $f(x) = 0$ for all $x$ if and only if $c = Tr_{n/\ell}(\delta) = 0$.

(c) Let $|C_{s_i}| = \ell_i$ where $\ell_i \leq n$, for any $i \in I$. We consider here

$$f(x) = \sum_{i \in I} \alpha_i \, Tr(\delta_i x^{s_i}) + c = \sum_{i \in I} \alpha_i \, Tr_{\ell_i/1}\left(Tr_{n/\ell_i}(\delta)x^{s_i}\right) + c.$$

Since the $s_i$ are from different cyclotomic cosets all the exponents in $f(x)$ are different. As previously, $f(x) = 0$ for all $x$ if and only if all coefficients of the $x^{s_i p^j}$ are zero. Since the functions $Tr(\delta_i x^{s_i})$ are not zero, this is equivalent to $\alpha_i = 0$ for all $i$. □

CLAIM 4. *Let $1 \leq t \leq p^n - 1$.*

(a) *Let $b$ be a nonzero element from $\mathbb{F}_{p^n}$. Then $x^t = b$ has a solution in $\mathbb{F}_{p^n}$ if and only if $b$ is a $t$-th power in $\mathbb{F}_{p^n}$.*

(b) *Let $u$ be a primitive element of $\mathbb{F}_{p^n}$ and $t$ be a divisor of $p^n - 1$. Then a nonzero element $b$ of $\mathbb{F}_{p^n}$ is a $t$-th power in $\mathbb{F}_{p^n}$ if and only if $b = u^r$ with $r$ divisible by $t$.*

(c) *A non-zero element $b$ of $\mathbb{F}_{p^n}$ is a $t$-th power in $\mathbb{F}_{p^n}$ if and only if $b^{(p^n-1)/d} = 1$, where $d = \gcd(p^n - 1, t)$.*

(d) *Let $p$ be odd and $1 \leq i \leq n - 1$. Then the equation $x^{p^i - 1} = -1$ has a solution in $\mathbb{F}_{p^n}$ if and only if $n/gcd(n, i)$ is even.*

PROOF. Statements (a)-(c) are obviously true. To prove (d), let $k = \gcd(i, n)$ and $n = k \cdot v$. Then $\gcd(p^i - 1, p^n - 1) = p^k - 1$ and $p^n - 1 = (p^k - 1)(p^{k(v-1)} + \cdots + p^k + 1)$. By (a) and (c) the equation $x^{p^i - 1} = -1$ is solvable in $\mathbb{F}_{p^n}$ if and only if

$$(-1)^{p^{k(v-1)} + \cdots + p^k + 1} = 1.$$

The latter is satisfied if and only if $p^{k(v-1)} + \cdots + p^k + 1$ is even or, equivalently, if the number $v$ of its summands is even. □

Now we are ready to characterize the monomial functions $Tr(\delta x^s)$ having a linear structure. This problem was partially solved by the second author for the case $|C_s| = n$ in [**9**]. Below, we rewrite Lemma 2 from [**9**] using Claim 2,(b).

LEMMA 2. *Let $0 \leq s \leq p^n - 2$ be of Hamming weight larger than 2 and $|C_s| = n$. Then the function $Tr(\delta x^s)$ has no linear structure for any nonzero $\delta \in \mathbb{F}_{p^n}$.*

Further we consider the cases which are not covered by Lemma 2.

LEMMA 3. *Let $s = k \cdot p^i$, where $0 < k \leq p - 1$ and $0 \leq i \leq n - 1$. Then the function $Tr(\delta x^s)$, $\delta \in \mathbb{F}_{p^n}^*$, has a linear structure if and only if $k = 1$.*

PROOF. Note that the statement of this lemma is independent on the choice of $\delta$. Therefore using Claim 2 we may without loss of generality assume that $i = 0$ and limit a linear structure to the element $1 \in \mathbb{F}_{p^n}$. It holds

$$(x+1)^k - x^k = \sum_{j=0}^{k-1} \binom{k}{j} x^j.$$

Clearly, different $0 \le j \le p-1$ belong to different cyclotomic cosets, and any such $j$ satisfies $\binom{k}{j} \not\equiv 0 \pmod p$. Hence by Claim 3,(c),

$$Tr\left(\delta((x+1)^k - x^k)\right) = \sum_{j=0}^{k-1} \binom{k}{j} Tr(\delta x^j)$$

is a constant function (equals to $Tr(\delta)$) if and only if $k = 1$. □

LEMMA 4. *Let $s = kp^i + mp^j$, where $0 < k, m \le p-1$ and $0 \le i < j \le n-1$. Assume that $|C_s| = n$ and $Tr(\delta x^s)$, $\delta \in \mathbb{F}_{p^n}^*$, is nonzero. Then the function $Tr(\delta x^s)$ has a linear structure only if $k = m = 1$.*

PROOF. Recall that notation $\prec$ is defined by (4). Claim 2 allows us to restrict ourselves to $i = 0$ and the linear structure 1. So, let $s = k + mp^j$. By Lucas Theorem, it holds

$$(x+1)^{k+mp^j} - x^{k+mp^j} = \sum_{t \prec s} \binom{k+mp^j}{t} x^t,$$

Any integer $t$ such that $t \prec s$ is as follows:

$$t = t_0 + t_j p^j \text{ where } 0 \le t_0 \le k \ , 0 \le t_j \le m \text{ and } t \ne k + mp^j.$$

We divide the last sum into three parts with respect to $t_j = 0$, $t_0 = 0$ and the rest denoted by $S$:

$$\sum_{t \in T} \binom{k+mp^j}{t} x^t = \sum_{t_0=1}^{k} \binom{k}{t_0} x^{t_0} + \sum_{t_j=1}^{m} \binom{m}{t_j} x^{t_j p^j} + S.$$

Now, we compute $f(x) = Tr(\delta((x+1)^s - x^s))$:

$$f(x) = \sum_{t_0=1}^{k} \binom{k}{t_0} Tr(\delta x^{t_0}) + \sum_{t_j=1}^{m} \binom{m}{t_j} Tr(\delta x^{t_j p^j}) + Tr(\delta S).$$

Suppose $m \ne k$, and w.l.g. $m > k$. Then in the above sum the only exponent belonging to $C_m$ is $mp^j$. Hence by Claim 3 this sum cannot be constant.

So let $k = m \ne 1$. Then $f(x)$ contains the summand $k\,Tr(\delta x^{k-1+kp^j})$. The assumption $|C_s| = n$ ensures $j \ne n/2$, and therefore $k-1+kp^j$ is the only exponent from its cyclotomic coset present in $f(x)$. Again by Claim 3 the function $f(x)$ cannot be constant. □

In the following lemma, we consider the exponents $s$ such that $|C_s| < n$. Recall that such integers have base $p$ representations of period $\ell$. This observation is helpful for the next proof.

LEMMA 5. *Let $1 \le s \le p^n - 2$ and $|C_s| < n$. Further let $\delta \in \mathbb{F}_{p^n}^*$ define a nonzero function $Tr(\delta x^s)$. Then $Tr(\delta x^s)$ has no linear structure.*

PROOF. Let $|C_s| = \ell$, $n = \ell m$ and $s = (s_{n-1} \dots s_0)_p$. We assume that $1 < \ell < n$; so we have implicitly $n \geq 4$ and $s > 2$.

By Claim 2 we may assume that $s$ is the smallest element of $C_s$ so that $s_0 \neq 0$. Moreover it is enough to show that $1 \in \mathbb{F}_{p^n}^*$ is not a linear structure of $Tr(\delta x^s)$ for an arbitrary $\delta$. Using Lucas Theorem we get

$$Tr\left(\delta\left((x+1)^s - x^s\right)\right) = \sum_{t \prec s} \binom{s}{t} Tr(\delta x^t). \tag{6}$$

Further, because of the $\ell$-periodic structure of $s$, if $t \prec s$ then $tp^{j\ell} \prec s$ for any $1 \leq j \leq m-1$ as well. After collecting all such exponents together, (6) is reduced to

$$\begin{aligned} Tr\left(\delta\left((x+1)^s - x^s\right)\right) &= \sum_{t \in T} \binom{s}{t} Tr\left((\delta + \delta^{p^\ell} + \dots + \delta^{p^{\ell(m-1)}})x^t\right) \\ &= \sum_{t \in T} \binom{s}{t} Tr\left(Tr_{n/\ell}(\delta)x^t\right), \end{aligned}$$

where $T$ is a set of representatives of the classes $\{t,\ tp^\ell, \dots,\ tp^{(m-1)\ell}\}$ with $t \prec s$.

Now we consider the summand corresponding to the exponent $s-1$. Note that $s-1 \prec s$, since $s_0 \neq 0$, and $|C_{s-1}| = n$, by Proposition 2. Moreover there is only one element from $C_{s-1}$ in $T$. Indeed, suppose that there is $0 < i < \ell$ such that $p^i(s-1) \in T$. Let $0 \leq \kappa \leq p^n - 2$ and $\kappa \equiv p^i(s-1) \pmod{p^n - 1}$. Since the multiplication by $p^i$ results a shift of the base $p$ representation, we have

$$\kappa = \kappa' - p^i,$$

where $\kappa' = p^i s \pmod{p^n - 1}$ with $0 \leq \kappa' \leq p^n - 2$. From the assumption $\kappa \in T$, it follows that $\kappa = \kappa' - p^i \prec s$. On the other hand $s < \kappa'$, since $s$ was chosen to be the smallest element of $C_s$. Hence there is $j$ such that $s_j < \kappa'_j$. Since the base $p$ representations of $s$ and $\kappa'$ are of period $\ell$, we can choose $j \geq \ell$, and in particular $j \neq i$. Then we have

$$s_j < \kappa'_j = (\kappa' - p^i)_j \leq s_j$$

a contradiction.

Hence by Claim 3 the function $Tr\left(\delta\left((x+1)^s - x^s\right)\right)$ is constant only if the summand $Tr\left(Tr_{n/\ell}(\delta)x^{s-1}\right)$ is constantly zero, which forces $Tr_{n/\ell}(\delta)$ to be zero. But we have

$$Tr(\delta x^s) = Tr_{\ell/1}\left(Tr_{n/\ell}(\delta)x^s\right)$$

since $x^s \in \mathbb{F}_{p^\ell}$. We conclude that for such a $\delta$ the function $Tr(\delta x^s)$ is the zero one, completing the proof. □

The next theorem characterizes the monomial functions assuming a linear structure. Moreover it specifies the linear structures of such functions. Note that a large part of (ii) in Theorem 5 follows also from the well known results in coding theory on computing the weights of the Reed-Muller codes of order 2 (see [**13, 14**]).

THEOREM 5. *Let $p$ be any prime number, $\delta \in \mathbb{F}_{p^n}$ and $1 \leq s \leq p^n - 2$ be such that $f(x) = Tr(\delta x^s)$ is not the zero function. Then $f$ has a linear structure if and only if one of the following cases occurs:*

**(i):** *$s = p^j$, $0 \leq j \leq n-1$, and $\delta \in \mathbb{F}_{p^n}^*$. In this case any $\alpha \in \mathbb{F}_{p^n}^*$ is a $Tr(\delta\alpha^s)$-linear structure of $f$.*

**(ii):** *$s = p^j(p^i+1)$, where $0 \le i,j \le n-1$, $i \notin \{0, n/2\}$. In this case, $\alpha \in \mathbb{F}_{p^n}$ is a linear structure of $f$ if and only if it satisfies*

$$\left(\delta^{p^{n-j}}\alpha^{p^i+1}\right)^{p^i-1} + 1 = 0.$$

*More exactly the linear space $\Lambda$ of $f$ is as follows:*

(a) *Let $p = 2$, $\tau = \gcd(n, 2i)$. Then $\Lambda = \{0\}$ if $\delta$ is not a $(2^i+1)$-th power in $\mathbb{F}_{2^n}$. Otherwise, if $\delta = \beta^{2^j(2^i+1)}$ for some $\beta \in \mathbb{F}_{2^n}$, it holds $\Lambda = \beta^{-1}\mathbb{F}_{2^\tau}$.*

(b) *Let $p$ be odd and $t = \gcd(n, i)$. Then $\Lambda \neq \{0\}$ if and only if $n/t$ is even and $\delta$ is as follows:*
- *$\delta$ is a $(p^t+1)$-th power in $\mathbb{F}_{p^n}$ if $n/2t$ is even;*
- *$\delta$ is a $(p^t+1)/2$-th power but not a $(p^t+1)$-th power in $\mathbb{F}_{p^n}$ if $n/2t$ is odd.*

*In this case $\Lambda$ consists of 0-linear structures, and $\Lambda = \epsilon\mathbb{F}_{p^{2t}}$ with $\epsilon$ satisfying $\left(\delta^{p^{n-j}}\epsilon^{p^i+1}\right)^{p^i-1} + 1 = 0$.*

Proof. By Lemmas 2–5 if $f$ has a linear structure then $s = p^j$ or $s = p^j(p^i+1)$ with $i \notin \{0, n/2\}$. Note that in both cases $|C_s| = n$, and hence $f$ is not the zero function for such an exponent and any nonzero $\delta$, according to Claim 3, (a).

**(i)** This case easily follows from the observation that $Tr(\delta x^{p^j}) = Tr(\delta^{p^{n-j}}x)$ is a linear function.

**(ii)** Let $s = p^j(p^i+1)$ and $i \notin \{0, n/2\}$. Claim 2,(a), shows that $\alpha \in \mathbb{F}_{p^n}^*$ is a linear structure of $Tr(\delta x^{p^j(p^i+1)})$ if and only if it is a linear structure of $Tr(\delta^{p^{n-j}}x^{p^i+1})$. Claim 2,(b), implies that $\alpha$ is a linear structure of $Tr(\delta^{p^{n-j}}x^{p^i+1})$ if and only if 1 is a linear structure of $Tr(\delta^{p^{n-j}}\alpha^{p^i+1}x^{p^i+1})$. Set $\mu = \delta^{p^{n-j}}\alpha^{p^i+1}$. Then we have

$$Tr(\mu((x+1)^{p^i+1} - x^{p^i+1})) = Tr(\mu(x^{p^i} + x + 1)) = Tr((\mu^{p^{n-i}} + \mu)x + \mu),$$

which is constant on $\mathbb{F}_{p^n}$ if and only if $\mu^{p^{n-i}} + \mu = 0$ or, equivalently, $\mu^{p^i} + \mu = 0$. Thus $\alpha$ is a linear structure of $f$ if and only if $\mu^{p^i-1} = -1$ where $\mu = \delta^{p^{n-j}}\alpha^{p^i+1}$. So the problem is reduced to the existence of $\alpha \in \mathbb{F}_{p^n}^*$ satisfying

$$\alpha^{p^{2i}-1} = -\left(\frac{1}{\delta^{p^{n-j}}}\right)^{p^i-1}. \tag{7}$$

Set $t = \gcd(n, i)$ and $\tau = \gcd(n, 2i)$.

Let $p = 2$. Then by Claim 4,(a), there is a solution of (7) if and only if $\delta^{2^{n-j}} = \beta^{2^i+1}$ for some $\beta \in \mathbb{F}_{2^n}^*$. In this case, clearly $\beta^{-1}$ satisfies (7) and thus $\Lambda = \beta^{-1}\mathbb{F}_{2^\tau}$.

For the rest of the proof we assume that $p$ is odd. Since a solution of (7) yields an element $\mu$ satisfying $\mu^{p^i-1} = -1$, Claim 4,(c), forces $n/\gcd(n,i) = n/t$ to be even. So, let $n/t$ be even. Then

$$\gcd(p^n - 1, p^{2i} - 1) = p^{\gcd(n,2i)} - 1 = p^{2t} - 1.$$

By Claim 4,(a),(c), there exists $\alpha \in \mathbb{F}_{p^n}^*$ satisfying (7) if and only

$$\left(-\left(\frac{1}{\delta^{p^{n-j}}}\right)^{p^i-1}\right)^{\frac{p^n-1}{p^{2t}-1}} = 1,$$

equivalently, if and only if

$$\left(-\delta^{(p^t-1)}\right)^{\frac{p^n-1}{p^{2t}-1}} = 1. \tag{8}$$

As in proof of Claim 4 mentioned, $(-1)^{\frac{p^n-1}{p^{2t}-1}} = 1$ if and only if $n/2t$ is even. Suppose that $n/2t$. Then (8) is reduced to

$$\left(\delta^{(p^t-1)}\right)^{\frac{p^n-1}{p^{2t}-1}} = \delta^{\frac{p^n-1}{p^t+1}} = 1,$$

implying that $\delta$ is a $(p^t+1)$-th power in $\mathbb{F}_{p^n}$.

If $n/2t$ is odd, then $(-1)^{\frac{p^n-1}{p^{2t}-1}} = -1$ and (8) is reduced to

$$\delta^{\frac{p^n-1}{p^t+1}} = -1 \implies \delta^{2\frac{p^n-1}{p^t+1}} = 1,$$

implying that $\delta$ is a $((p^t+1)/2)$-th power but not a $(p^t+1)$-th power in $\mathbb{F}_{p^n}$.

Note that if $\epsilon \in \mathbb{F}_{p^n}$ is a solution of (7), then $\Lambda = \epsilon\mathbb{F}_{p^{2t}}$. To complete the proof it remains to show that every $\alpha \in \Lambda^*$ is a 0-linear structure of $f$. By definition of a linear structure it follows that $\alpha$ is an $f(\alpha)$-linear structure of $f$. We have

$$f(\alpha) = Tr(\delta\alpha^{p^j(p^i+1)}) = Tr(\delta^{p^{n-j}}\alpha^{p^i+1}).$$

Let $u \in \mathbb{F}_p^*$. Then $u\alpha \in \Lambda^*$ and it is a $u^2f(\alpha)$-linear structure of $f$, since

$$f(u\alpha) = Tr(\delta^{p^{n-j}}(u\alpha)^{p^i+1}) = u^2Tr(\delta^{p^{n-j}}\alpha^{p^i+1}) = u^2f(\alpha).$$

On the other hand, by Proposition 1 the element $u\alpha$ is a $uf(\alpha)$-linear structure of $f$. Hence it must hold $u^2f(\alpha) = uf(\alpha)$ for any $u \in \mathbb{F}_p$, and therefore $f(\alpha) = 0$ for any $\alpha \in \Lambda^*$. □

REMARK 1. *Let $p = 2$. Consider $f(x) = Tr(\delta x^{2^j(2^i+1)})$ with $i \notin \{0, n/2\}$. It is well-known that*

$$\gcd(2^i+1, 2^n-1) = 1 \;\Leftrightarrow\; \gcd(i,n) = \gcd(2i,n),$$

*which is especially true when $n$ is odd. Thus for such $i$ and $n$ every non-zero element of $\mathbb{F}_{2^n}$ is a $2^i+1$-power. Then Theorem 5, (ii), shows that for any $\delta \in \mathbb{F}_{2^n}^*$ the linear space of $f$ is not trivial.*

Theorems 2 and 5 yield the following family of sparse permutation polynomials.

THEOREM 6. *Let $0 \le i \le n-1$, $i \notin \{0, n/2\}$ and $\gamma, \delta \in \mathbb{F}_{p^n}$ be such that*

$$\left(\delta\gamma^{p^i+1}\right)^{p^i-1} + 1 = 0.$$

*Then*

$$F(X) = X + \gamma\, Tr(\delta X^{p^i+1})$$

*is a permutation polynomial of $\mathbb{F}_{p^n}$ whenever*

- *$p$ is odd*
- *$p = 2$ and $Tr(\delta\gamma^{p^i+1}) = 0$.*

*Moreover, if $p = 2$ and $Tr(\delta\gamma^{p^i+1}) = 1$, then $F(X)$ induces a $2-to-1$ mapping on $\mathbb{F}_{2^n}$.*

## 4. Properties of mappings $\mathbf{x^s + \gamma\, Tr(x^t)}$

In this section we indicate some properties of the mappings

$$x \mapsto x^s + \gamma\, Tr(x^t),\ x \in \mathbb{F}_{2^n},$$

which are relevant for cryptological applications. Let us repeat briefly some basic facts. Any mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is given by a polynomial over $\mathbb{F}_{2^n}$ of degree less than $2^n$. The algebraic degree of the mapping $F(x) = \sum_{k=0}^{2^n-1} \alpha_k x^k$ is $\max_{k,\alpha_k \neq 0}\{\mathrm{wt}(k)\}$, where $\mathrm{wt}(k)$ is the binary weight of $k$. For any $a$ and $b$ in $\mathbb{F}_{2^n}$, we define

$$\delta_F(a,b) = |\{x \in \mathbb{F}_{2^n},\ F(x) + F(x+a) = b\}|$$

and

$$\delta(F) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \delta_F(a,b).$$

A mapping $F$ is said to be *differentially $k$-uniform* if $\delta(F) = k$. It is easy to see that $\delta(F) \geq 2$. A mapping $F$ is called *almost perfect nonlinear (APN)* if $\delta(F) = 2$. More details on this context can be found, for instance, in [**1, 8**].

To protect a block cipher against attacks the involved mappings must be permutations having large algebraic degree and low differential uniformity. Moreover, these mappings must be represented by sparse polynomials to admit an efficient implementation. The "inverse" mapping $x \mapsto x^{2^n-2}$ permutes $\mathbb{F}_{2^n}$ and has algebraic degree $n-1$. It is APN if $n$ is odd, and it is differentially 4-uniform if $n$ is even. The inverse mapping is used as the S-box of AES for $n = 8$. The existence of APN permutations for even $n$ was (and it is still) the mystery of the research on APN mappings, until the recent announcement of such mappings for $n = 6$ by John Dillon [**7**].

The use of monomial mappings in block ciphers is often criticized, since such mappings exploit only the multiplicative structure of the underlying finite field. Define

$$F_{s,t,\gamma}(X) = X^s + \gamma\, Tr(X^t), \tag{9}$$

where $1 \leq s, t \leq 2^n - 2$ and $\gamma \in \mathbb{F}_{2^n}^*$. In the rest of this section we will show that for certain choices of $s, t, \gamma$ the mapping $F_{s,t,\gamma}$ is a permutation with large algebraic degree and low differential uniformity.

Firstly we characterize $s, t, \gamma$ such that the corresponding $F_{s,t,\gamma}$ is a permutation of $\mathbb{F}_{2^n}$ (see also [**5**, Corollary 1]).

THEOREM 7. *Let $F_{s,t,\gamma}(X) = X^s + \gamma\, Tr(X^t)$ with $\gamma \in \mathbb{F}_{2^n}^*$. Then $F_{s,t,\gamma}$ is a permutation on $\mathbb{F}_{2^n}$ if and only if* $\gcd(s, 2^n - 1) = 1$,

$$t \equiv 2^j(2^i + 1)s \pmod{2^n - 1} \text{ for some } 0 \leq i, j \leq n-1,\ i \neq n/2,$$

*and either (a) or (b) holds:*

(a) $i = 0$ *and* $Tr(\gamma) = 0$.

(b) $i > 0$ *and* $\gamma \in \mathbb{F}_{2^k}$ *with* $Tr(\gamma^{2^i+1}) = 0$, *where* $k = \gcd(2i, n)$.

*Moreover, if $Tr(\gamma) = 1$, in case (a), or $Tr(\gamma^{2^i+1}) = 1$ in case (b), then $F_{s,t,\gamma}$ is a 2-to-1 mapping.*

PROOF. Note that if $\gcd(s, 2^n - 1) > 2$, then $F_{s,t,\gamma}$ cannot be a permutation, since $Tr(x^t)$ is two valued. Hence $\gcd(s, 2^n - 1) = 1$, implying that $x \mapsto x^s$ is a permutation. Let $s^{-1}$ be the inverse of $s$ modulo $2^n - 1$. By Theorem 3 the mapping $F_{s,t,\gamma}$ is a permutation if and only if $\gamma$ is a 0-linear structure of $Tr(x^{ts^{-1}})$. Using

Theorem 5, this is possible if and only if $ts^{-1} \equiv 2^j(2^i+1)$ modulo $2^n-1$, for some $i, j$. To complete the proof it remains to note, that case (a) corresponds to case **(i)** of Theorem 5. Further, (b) follows from case **(ii)**(a) of Theorem 5: In this case $Tr(x^{ts^{-1}}) = Tr(x^{2^i+1})$ and $\gamma$ is a $Tr(\gamma^{2^i+1})$-linear structure of $Tr(x^{2^i+1})$ if and only if $\gamma \in \mathbb{F}_{2^k}$. □

In [**3**] it was observed that any mapping $F(x) = G(x) + Tr(H(x))$ satisfies $\delta(F) \leq 4$ as soon as $G$ is APN. We give in the next proposition a slightly more general version of this fact.

PROPOSITION 3. *Let $G$ and $H$ be mappings on $\mathbb{F}_{2^n}$ and $\delta(G) = \rho$. Then the mapping $F(x) = G(x) + \gamma Tr(H(x))$ satisfies $\delta(F) \leq 2\rho$ for any $\gamma \in \mathbb{F}_{2^n}^*$.*

PROOF. Let $a \in \mathbb{F}_{2^n}$. Then

$$F(x) + F(x+a) = G(x) + G(x+a) + \gamma\epsilon,$$

where $\epsilon = Tr(H(x) + H(x+a)) \in \mathbb{F}_2$. This shows that for any $a, b \in \mathbb{F}_{2^n}$, it holds

$$\delta_F(a,b) \leq \delta_G(a,b) + \delta_G(a, b+\gamma) \leq 2\rho,$$

implying the proof. □

Combining Theorem 7 and Proposition 3, we obtain an infinite class of sparse polynomials describing permutations with upper bounded differential uniformity.

COROLLARY 1. *Let $\gcd(s, 2^n-1) = 1$ and the permutation $x \mapsto x^s$ be differentially $\rho$-uniform. Further, let $1 \leq i < n/2$ and $k = \gcd(2i, n)$. Then for any $\gamma \in \mathbb{F}_{2^k}$ such that $Tr(\gamma^{2^i+1}) = 0$ the polynomial*

$$F_{s,s(2^i+1),\gamma}(X) = X^s + \gamma\, Tr\left(X^{s(2^i+1)}\right)$$

*defines a permutation on $\mathbb{F}_{2^n}$ satisfying $\delta\left(F_{s,s(2^i+1),\gamma}\right) \leq 2\rho$.*

We conclude this section with some remarks on the permutations $F_{s,t,\gamma}$ with low differential uniformity. We use the notation $f_s : x \mapsto x^s$.

It is well known that if $f_s$ is APN then $\gcd(s, 2^n-1) = 1$ when $n$ is odd and $\gcd(s, 2^n-1) = 3$ when $n$ is even (see [**1**, Proposition 3]). Using Claim 1 or Theorem 7 we observe that

> *There is no permutation of the shape $X^s + \gamma\, Tr(X^t)$ with $n$ even and $x \mapsto x^s$ is APN.*

For an odd $n$, we derive another observation on $F_{s,s(2^i+1)}$ from Theorem 7. If $\gcd(2i, n) = 1$ then $\gamma$ must be chosen from $\mathbb{F}_2$. Since $Tr(1) = 1$, we cannot obtain permutations for such $i$. Thus

> *There is no permutation of the shape $X^s + \gamma\, Tr(X^{s(2^i+1)})$ with $n$ odd and $\gcd(i, n) = 1$.*

However, such permutations exist whenever $n$ is an odd composed number. As was noticed in Corollary 1, we exhibit a large class of permutations which are at most differentially $2\rho$-uniform as soon as $f_s$ is differentially $\rho$-uniform. In particular, when $f_s$ is APN we get permutations which are at most differentially 4-uniform. In the next proposition we apply these ideas to the *inverse* mapping and obtain permutations with low differential uniformity and large algebraic degree.

PROPOSITION 4. *Let $\gamma \in \mathbb{F}_{2^n}^*$, $0 \leq i < n, i \neq n/2$, and*

$$G_{i,\gamma}(X) = X^{2^n-2} + \gamma\, Tr(X^{2^{n-1}-2^{i-1}-1}). \tag{10}$$

*Then $G_{i,\gamma}(X)$ is a permutation polynomial if either* **(i)** *or* **(ii)** *holds:*

**(i):** *$i = 0$ and $Tr(\gamma) = 0$ (a trivial case).*

**(ii):** *$0 < i < n$, $i \neq n/2$ and $\gamma \in \mathbb{F}_{2^k}$ such that $Tr(\gamma^{2^i+1}) = 0$, where $k = \gcd(2i, n)$. Moreover, $\delta(G_{i,\gamma}) \leq 4$ for odd $n$ and $\delta(G_{i,\gamma}) \leq 8$ for even $n$.*

PROOF. Recall that the inverse mapping is APN for odd $n$ and differential 4-uniform for even $n$. The upper-bound on $\delta(G_{i,\gamma})$ is obtained by Proposition 3.

The case $i = 0$ corresponds to Theorem 7, (a). Note that $G_{0,\gamma}$ is a composition of the linear permutation $X + \gamma Tr(X)$ and the inverse mapping, and therefore the differential uniformity of $G_{0,\gamma}$ is equal to the one of the inverse mapping.

The case $i > 0$ follows from Corollary 1, since

$$\begin{aligned}(2^n-2)(2^i+1) &= 2^i + 2^n - 2^{i+1} - 2 = 2^n - 2^i - 2 \\ &= 2(2^{n-1} - 2^{i-1} - 1) \pmod{2^n - 1}.\end{aligned}$$

□

Clearly, the mappings which are *at most* differentially 4-uniform must be checked whether they are APN. Presently only APN mappings of algebraic degree 2 of the shape $x^s + Tr(x^t)$ are known. Notably the mapping $x \mapsto x^3 + Tr(x^9)$ is APN for any $n$ [**3**]. Using the previous discussions it is clear that they cannot be permutations:

*There is no permutation on $\mathbb{F}_{2^n}$ of the shape $X^3 + \gamma\, Tr(X^9)$, for any $\gamma \in \mathbb{F}_{2^n}^*$ and for any $n$.*

## 5. Conclusion

In this paper we focused on the simplest permutations that can be constructed using the tools described in [**5, 6**]. To do that we completely solved the problem of the existence of linear structures of monomial functions. The characterization of all polynomials yielding functions with linear structure remains open in general. The results from [**2**] yield some partial information for binomial functions. For any solved instance of this problem Theorem 2 allows to construct permutation polynomials.

Another open problem is the determination of the Walsh spectrum of the considered permutations. Little is known about the Walsh spectrum of $F_{s,t,\gamma}$ considered in Corollary 1. We think that some insight on this problem can be obtained using the tools of [**1**]. In general, any property linking the mappings $f_s$ and $F_{s,t,\gamma}$ is of great interest.

## References

[1] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Trans. Inform. Theory*, 52(9):4160–4170, September 2006.

[2] J. Bierbrauer and G. Kyureghyan, Crooked binomials, Des. Codes Cryptogr. 46 (2008) 269-301.

[3] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN from known ones, Finite Fields Appl. 15(2) (2009) 150-159.

[4] A. Canteaut and M. Naya-Plasencia, Structural weakness of mappings with a low differential uniformity, Conference on Finite Fields and Applications, Dublin, July 13-17 2009.

[5] P. Charpin and G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368-376.
[6] P. Charpin and G. Kyureghyan, When does $G(x)+\gamma\, Tr(H(x))$ permute $\mathbb{F}_{p^n}$ ? Finite Fields Appl., 15(5) (2009) 615-632.
[7] J. Dillon, APN polynomials: An Update. Invited talk at Fq9, the *9th International Conference on Finite Fields and Applications*, Dublin, July 13-17 2009.
[8] Y. Edel and A. Pott, A new perfect nonlinear function which is not quadratic, Adv. in Math. of Communications 3(1) (2009) 59-81.
[9] G. Kyureghyan, Crooked maps in $F_{2^n}$, Finite Fields Appl. 13(3) (2007) 713-726.
[10] G. Kyureghyan, Constructing permutations of finite fields via linear translators, submitted, available on arXiv:0903.0743.
[11] X. Lai, Additive and linear structures of cryptographic functions, FSE 94, in: Lecture Notes in Comput. Sci., vol. 1008, Springer Verlag, Berlin, 1995, pp. 75-85.
[12] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983.
[13] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer, Boston, 1987.
[14] R.J. McEliece, Quadratic forms over finite fields and second order Reed-Muller codes, JPL Space Programs Summary, 37-58-III (1969) 28-33.

INRIA, SECRET research Team, B.P. 105, 78153 Le Chesnay Cedex, France
*E-mail address*: Pascale.Charpin@inria.fr

Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany.
*E-mail address*: Gohar.Kyureghyan@Mathematik.Uni-Magdeburg.DE