Quadratic functions with prescribed spectra

Wilfried Meidl, Alev Topuzoglu

Quadratic functions with prescribed spectra

Wilfried Meidl and Alev Topuzoğlu

Sabancı University MDBF, Orhanlı, Tuzla, 34956 Istanbul, Turkey
`wmeidl@sabanciuniv.edu`, `alev@sabanciuniv.edu`

Abstract. We study quadratic Boolean functions f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, which are well-known to have plateaued Fourier spectrum $\mathcal{F}_{s,f}$, i.e., their Fourier coefficients are in the set $\{0, \pm 2^{(n+s)/2}\}$ for some integer $0 \le s \le n-1$. For various types of integers n, we determine possible values of s, construct f with $\mathcal{F}_{s,f}$ for a prescribed s, and present enumeration results in case n is a power of 2.
Our work generalizes some of the earlier results of Khoo et. al. ([5]) on near-bent functions and provides a simple proof of a result of Fitzgerald ([2]) on degenerate quadratic forms.

Keywords: Quadratic Boolean functions, s-plateaued functions, near-bent functions, self-reciprocal polynomials, linear complexity

1 Introduction

We study quadratic functions

$$f(x) = \mathrm{Tr_n}\left(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^{2^i+1}\right) \tag{1}$$

from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, with coefficients in $\mathbb{F}_2$.

It is well known that any quadratic function is *plateaued* i.e., it has (plateaued) Fourier spectrum

$$\mathcal{F}_{s,f}$$

, in other words, its Fourier coefficients lie in $\{0, \pm 2^{(n+s)/2}\}$ for some integer $0 \le s \le n-1$. In this case we call f *s-plateaued.* 1-plateaued functions have been widely studied, and are called *near-bent* or *semi-bent* (when n is odd), see for instance [1, 6].

One of the problems, that [5] focuses on, is to characterize integers n, for which all f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ of the form (1) are near-bent.

The more general question we address here is the following: Given an integer n, characterize those integers s, for which s-plateaued functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ of the form (1) exist. We obtain the characterization when n is a square-free integer or is a power of 2. For these classes of integers n, we give methods for constructing s-plateaued functions for all possible s. We also enumerate the s-plateaued functions in case $n = 2^m$, $m \geq 1$.

Using standard Welch-squaring techniques one can see that the integer s is the dimension over $\mathbb{F}_2$ of the kernel of the linear transformation defined on $\mathbb{F}_{2^n}$ by

$$L(x) = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} \left(a_i x^{2^i} + a_i^{2^{n-i}} x^{2^{n-i}} \right),$$

i.e., $\gcd(x^{2^n} + x, L(x))$ has degree 2^s. Equivalently $ker(L)$ has dimension s if and only if the associates $A(x)$ and $x^n + 1$ of $L(x)$ and $x^{2^n} + x$, respectively, satisfy (see [7, p.118])

$$\deg(\gcd(A(x), x^n + 1)) = s.$$

The associate $A(x)$ corresponding to f in (1) is

$$A(x) = \sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^i + a_i x^{n-i} = x^{i_0} g(x), \tag{2}$$

where i_0 is the smallest integer such that $a_{i_0} \neq 0$, and $g(x) \in \mathbb{F}_2[x]$ is the self-reciprocal polynomial

$$g(x) = \sum_{i=i_0}^{\lfloor (n-1)/2 \rfloor} a_i (x^{i-i_0} + x^{n-i_0-i})$$

of degree $n - 2i_0$.

Note that $\gcd(\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} a_i x^i + a_i x^{n-i}, x^n + 1) = \gcd((\sum_{i=1}^{\lfloor (n-1)/2 \rfloor} a_i x^i + a_i x^{n-i}) + a_0(x^n + 1), x^n + 1)$, i.e., a_0 does not effect the value of s. Hence we can suppose that the degree of $A(x)$ is at most $n - 1$.

We recall that the linear complexity $L(S)$ of an n-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_2$ is determined by

$$L(S) = n - \deg(\gcd(x^n + 1, S(x)))$$

where $S(x)$ is the *generating polynomial* of S, i.e., the polynomial of degree at most $n-1$ given by $S(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}$. Therefore the calculation of the values in the Fourier spectrum of a quadratic function (1) is equivalent to the determination of the linear complexity of an n-periodic sequence with generating polynomial of the form (2). More precisely $s = n - L$ if L is the linear complexity of the corresponding n-periodic sequence.

2 Main Results

2.1 The case $n = 2^m$

In this subsection we will employ the well known Games-Chan algorithm (see [3]) to enumerate the functions (1) from $\mathbb{F}_{2^{2^m}}$ to $\mathbb{F}_2$ that yield s-plateaued functions. The algorithm also leads to a tool of constructing s-plateaued functions for a given s.

The following example describes how one can calculate s.

Example 1. For $m = 4$ consider $f(x) = \mathrm{Tr_n}(x^2 + x^3 + x^{2^4+1} + x^{2^5+1})$, then $A(x) = 1 + x + x^4 + x^5 + x^{11} + x^{12} + x^{15} + x^{16}$. For our purpose we consider this polynomial modulo $x^{16} + 1$ and put

$$A(x) = x + x^4 + x^5 + x^{11} + x^{12} + x^{15}$$

and obtain the corresponding 16-periodic binary sequence

$$S = (0100110000011001)^\infty.$$

$$\begin{array}{c} 0\,1\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,1 \\ \hline 0\,1\,0\,1\,0\,1\,0\,1 \\ L=8 \end{array} \qquad \begin{array}{c} 0\,1\,0\,1 \\ 0\,1\,0\,1 \\ \hline 0\,0\,0\,0 \\ L=8 \end{array}$$

$$\begin{array}{c} 0\,1 \\ 0\,1 \\ \hline 0\,0 \\ L=8 \end{array} \quad \begin{array}{c} 0 \\ 1 \\ \hline 1 \\ L=9 \end{array} \quad L = L + 1 = 10.$$

As the 16-periodic sequence S corresponding to $A(x)$ has linear complexity $L = 10$, the quadratic function f is s-plateaued with $s = 16 - 10 = 6$.

The Games-Chan algorithm motivates the definition of a mapping φ_m from $\mathbb{F}_2^{2^m}$ to $\mathbb{F}_2^{2^{m-1}}$, $m \geq 1$, as follows:

$$\varphi_m((s_0, s_1, \ldots, s_{2^m-1})) = (s_0 + s_{2^{m-1}}, s_1 + s_{2^{m-1}+1}, \ldots, s_{2^{m-1}-1} + s_{2^m-1}).$$

In the following proposition we collect some simple observations for 2^m-periodic sequences corresponding to polynomials $A(x)$ in (2) with $n = 2^m$. As remarked above we can assume that $a_0 = 0$, thus $\deg(A) \leq n - 1$. The strings $\mathbf{s}^{(m)} = s_0, s_1, \ldots, s_{2^m-1}$ of our interest can easily be seen to satisfy $s_0 = s_{n/2} = 0$, $s_i = s_{n-i}$, $i = 1, \ldots, n/2 - 1$. We will call a string satisfying these properties *antisymmetric*. Accordingly, we call the corresponding sequence antisymmetric 2^m-periodic sequence.

Proposition 1. *Let* $\mathbf{s}^{(m)} = s_0, s_1, \ldots, s_{2^m-1}$ *be a string,* $m \geq 1$*.*

(i) An antisymmetric string $\mathbf{s}^{(m)}$ *is determined by the bits* $s_1, \ldots, s_{2^{m-1}-1}$*. There are* $2^{2^{m-1}-1}$ *distinct antisymmetric strings of length* 2^m*.*

(ii) If $\mathbf{s}^{(m)}$ *is antisymmetric, then* $\varphi_m(\mathbf{s}^{(m)})$ *is also.*

(iii) The set of antisymmetric preimages $\varphi_m^{-1}(\mathbf{s}^{(m-1)})$ *of an antisymmetric string* $\mathbf{s}^{(m-1)}$ *has cardinality* $2^{2^{m-2}}$*.*

(iv) Let $\mathbf{s}^{(m)}$ *be an antisymmetric string satisfying* $\varphi_m(\mathbf{s}^{(m)}) = 0, 0, \ldots, 0$*. Then either* $s_0, s_1, \ldots, s_{2^{m-1}-1}$ *is itself antisymmetric, or the string*

$$s_0, s_1, \ldots, s_{2^{m-2}} + 1, \ldots, s_{2^{m-1}-1}$$

is antisymmetric.
In the first case $\varphi_{m-1}(s_0, s_1, \ldots, s_{2^{m-1}-1}) = t_0, t_1, \ldots, t_{2^{m-2}-1}$ *is antisymmetric, and in the second case the string* $t_0 - 1, t_1, \ldots, t_{2^{m-2}-1}$ *is antisymmetric.*

Theorem 1. *For* $n = 2^m$*, let* $\mathcal{N}_m(s)$ *denote the number of strings*

$$(a_1, a_2, \ldots, a_{(n/2)-1}) \in \mathbb{F}_2^{(n/2)-1}$$

for which the quadratic function f *from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_2$*, given by*

$$f(x) = \mathrm{Tr_n}\left(\sum_{i=1}^{(n/2)-1} a_i x^{2^i+1}\right)$$

is s*-plateaued. Then*

$$\mathcal{N}_m(s) = \begin{cases} 2^{2^{m-1}-1-k} & : \quad s = 2k, k = 1, \ldots, 2^{m-1}-1, \\ 0 & : \quad s = 0 \text{ or } s \text{ odd.} \end{cases}$$

Proof. We use induction. One can easily see that the assertion holds for small m. Now suppose that $\mathcal{N}_{m-1}(s) = 2^{2^{m-2}-1-k}$ for $s = 2k, k = 1, \ldots, 2^{m-2}-1$, i.e., for these values of s, there are $2^{2^{m-2}-1-k}$ sequences, which are 2^{m-1}-periodic with linear complexity $2^{m-1} - s$, corresponding to antisymmetric strings. By Proposition 1 (iii), for each of these stings we have $2^{2^{m-2}}$ antisymmetric preimages giving rise to antisymmetric 2^m-periodic sequences with linear complexity $2^m - s$. Proposition 1 (ii) implies that these are all such sequences. Consequently, we get $\mathcal{N}_m(s) = 2^{2^{m-2}} 2^{2^{m-2}-1-k} = 2^{2^{m-1}-1-k}$ when $s = 2k, k = 1, \ldots, 2^{m-2}-1$. It remains to show that the formula holds for $s = 2k$ with $k = 2^{m-2}, \ldots, 2^{m-1}-1$. We therefore have to enumerate the antisymmetric 2^m-periodic sequences with a given linear complexity $2^m - s \leq 2^{m-1}$. First observe that these are the sequences corresponding to antisymmetric strings $\mathbf{s}^{(m)} = s_0, \ldots, s_{2^m-1}$ such that
(a) $\varphi_m(\mathbf{s}^{(m)}) = 0, 0, \ldots, 0$, or
(b) the sequence corresponding to $s_0, \ldots, s_{2^{m-1}-1}$ has linear complexity $2^m - s$.
By Proposition 1 (iv), (a) implies that $s_0, \ldots, s_{2^{m-1}-1}$ or $s_0, s_1, \ldots, s_{2^{m-2}} +$

$1,\ldots,s_{2^{m-1}-1}$ is antisymmetric. Moreover it is easily seen that for any such string there is exactly one corresponding antisymmetric string $\mathbf{s}^{(m)}$ for which (a) holds. Having an odd number of 1's, the $2^{m-2}-1$ strings of the second type yield 2^{m-1}-periodic sequences with linear complexity $L = 2^{m-1}$ (thus $s = 2^m - L = 2^{m-1}$). Among the $2^{m-2}-1$ strings of the first type, by our hypothesis, precisely $2^{2^{m-2}-1-\kappa}$ yield 2^{m-1}-periodic sequences with linear complexity $L = 2^{m-1} - 2\kappa$, $\kappa = 1,\ldots,2^{m-2}-1$. Substituting κ by $k - 2^{m-2}$ we obtain $2^{2^{m-1}-1-k}$ for the number of antisymmetric 2^m-periodic sequences with linear complexity $L = 2^m - 2k$ (thus $s = 2k$) for $k = 2^{m-2}+1,\ldots,2^{m-1}-1$, hence $\mathcal{N}_m(s) = 2^{2^{m-2}}2^{2^{m-2}-1-k} = 2^{2^{m-1}-1-k}$ for these values of k, and $s = 2k$. Note that from the above arguments we also see that $\mathcal{N}_m(s) = 0$ when $s = 0$ and when s is odd. However one can also see directly that $\mathcal{N}_m(0) = 0$ since antisymmetric strings contain an even number of 1's, and the statement for odd s simply follows from the Fourier transform being an integer. □

Note that the arguments in the proof also enable the construction of s-plateaued quadratic functions from $\mathbb{F}_{2^{2^m}}$ to $\mathbb{F}_2$ for a prescribed value of s.

2.2 The case $n = p_1p_2\cdots p_r$

The results in this subsection are obtained with a different approach, namely by analysing the factorization of x^n+1 into self-reciprocal polynomials. With the observation that $\gcd(x^n+1, A(x))$ is again self-reciprocal if $A(x)$ is self-reciprocal, one obtains the following general theorem, which is valid for arbitrary integers n.

Theorem 2. *Let n be arbitrary.*

(i) If n is odd, then there exists an s-plateaued function of the form (1) *if and only if s is odd and x^n+1 has a self-reciprocal factor $h(x)$ of degree s (in which case x^n+1 is always divisible by $x+1$).*

(ii) If n is even then there exists an s-plateaued function of the form (1) *if and only if s is even and x^n+1 has a self-reciprocal factor $h(x)$ of degree s divisible by $(x+1)^2$.*

Note that if $n = 2^v n_1$, n_1 odd, then $x^n+1 = (x^{n_1}+1)^{2^v}$. Thus it is sufficient to analyse the factorization of x^n+1 for odd n. Here we only consider the case of n being square-free. Our main tool for studying the factorization of x^n+1 into self-reciprocals is, as expected, the use of cyclotomic cosets modulo n relative to powers of 2.

We denote the n-th cyclotomic polynomial by $\mathcal{Q}_n$, and denote the 2-adic valuation of an integer k by $\nu(k)$, i.e., $2^{\nu(k)}$ is the largest power of 2 which divides k. The following lemma describes for which squarefree integers $n = p_1p_2\cdots p_r$ the irreducible factors of $\mathcal{Q}_n$ are self-reciprocal. Note that $\mathcal{Q}_n$ has d irreducible factors where $d = \mathrm{lcm}(d_1,\ldots,d_r) = ord_n 2$.

Lemma 1. *Let* $n = p_1 p_2 \cdots p_r$, $d_i = ord_{p_i} 2$ *and* $d = ord_n 2$. *Suppose the irreducible factors of* $\mathcal{Q}_n$ *are* $f_1, \ldots, f_{\varphi(n)/d}$. *Then*

(i) The polynomials $f_1, \ldots, f_{\varphi(n)/d}$ *are self-reciprocal if and only if* $\nu(d_1) = \nu(d_2) = \cdots = \nu(d_r) > 0$. *In particular, if* n *is a prime* p, *then* $f_1, \ldots, f_{(p-1)/d}$ *are self-reciprocal if and only if* d *is even.*

(ii) If $\nu(d_i) \neq \nu(d_j)$ *for some* $1 \leq i, j \leq \varphi(n)/d$, *then none of the polynomials* f_t, $1 \leq t \leq \varphi(n)/d$, *is self-reciprocal, and for each* t, $1 \leq t \leq \varphi(n)/d$, *there exists a unique* $t' \neq t$, $1 \leq t' \leq \varphi(n)/d$ *such that the product* $f_t f_{t'}$ *is self-reciprocal.*

Idea of Proof. First observe that the irreducible factors of $\mathcal{Q}_n$ are self-reciprocal if every cyclotomic coset modulo n relative to powers of 2 containing the element a also contains the element $-a$. Therefore an irreducible factor of $\mathcal{Q}_n$ is self-reciprocal if the cyclotomic coset of 1 also contains -1, i.e., $2^k \equiv -1 \bmod n$ for some integer k. This is equivalent to $2^k \equiv -1 \bmod p_1$, $i \leq i \leq r$, which holds if and only if d_i divides $2k$ but not k for each i. This leads to the condition $\nu(d_1) = \nu(d_2) = \cdots = \nu(d_r) > 0$. □

By Lemma 1 and [7, Exercise 3.15] the polynomial $x^n + 1$ factors into self-reciprocal irreducible polynomials if and only $\nu(d_1) = \nu(d_2) = \cdots = \nu(d_r) > 0$.

Example 2. I. $n = 5 \cdot 13 = 65$, then $d_1 = 4, d_2 = 12$, hence $\nu(d_1) = \nu(d_2)$. Consequently $x^{65} + 1$ factors into self-reciprocal irreducible polynomials.

II. $n = 3 \cdot 5 \cdot 7 = 105$, then $d_1 = 2, d_2 = 4, d_3 = 3$ and $\nu(d_1) \neq \nu(d_2)$. Hence not all the irreducible factors of $x^{105} + 1$ are self-reciprocal.

A simple consequence of the above lemma is also the main result of [5]: All functions of the form (1) from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ are 1-plateaued (near-bent) only when $n = p$ is a prime, satisfying $p \equiv 3 \bmod 4$ with $ord_p 2 = (p-1)/2$, or 2 is a primitive root modulo p. Note that the self-reciprocal factors of $x^n + 1$ are exactly $x + 1$ and $1 + x \cdots + x^{n-1}$ only for such n.

In order to determine the possible values of s that a function of the form (1) has Fourier spectrum $\mathcal{F}_{s,f}$, we consider all cyclotomic polynomials $\mathcal{Q}_m$, $m|n$ and apply Lemma 1 accordingly:

Example 2.II. continued: $n = 3 \cdot 5 \cdot 7 = 105, d_1 = 2, d_2 = 4, d_3 = 3$.
$\varphi(n) = 48$, $d = \gcd(2, 4, 3) = 12$, and $\nu(d_1) \neq \nu(d_2)$. Hence $x^{105} + 1$ has 2 self-reciprocal factors of degree 24.
$\varphi(35) = 24$, $\gcd(d_2, d_3) = \gcd(4, 3) = 12$, and $\nu(4) \neq \nu(3)$, which yields 2 cyclotomic classes of cardinality 12, and hence one self-reciprocal factor of degree 24.
$\varphi(21) = 12$, $\gcd(2, 3) = 6$. There are 2 cyclotomic classes of cardinality 6 corresponding to one self-reciprocal factor of degree 12.
$\varphi(15) = 8$, $\gcd(2, 4) = 4$, $\nu(2) \neq \nu(4)$. There are 2 cyclotomic classes of cardinality 4, giving one self-reciprocal factor of degree 8.
Similarly it is easy to see that $x^{105} + 1$ has one self-reciprocal factor of degree 6, and two irreducible self-reciprocal factors; one of degree 4, and one of degree 2.

Therefore s can be any integer less than 105 of the form $s = 24k_1 + 12k_2 + 8k_3 + 6k_4 + 4k_5 + 2k_6 + 1$, $0 \le k_1 \le 3$ and $0 \le k_i \le 1$ for $2 \le i \le 6$.

We list the possible values of s in two special cases:

Corollary 1. *Let n be an odd prime with $ord_n 2 = d$.*

(i) If d is even, then there exists an s-plateaued function of the form (1) *from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ if and only if $s = kd + 1$ for some $0 \le k \le (n-1)/d - 1$.*

(ii) If d is odd, then there exists an s-plateaued function of the form (1) *from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ if and only if $s = 2kd + 1$ for some $0 \le k \le (n-1)/(2d) - 1$.*

Corollary 2. *Let $n = pq$ for two odd primes p and q and let $ord_p 2 = d_p$, $ord_q 2 = d_q$. The integers s for which there exists an s-plateaued function of the form* (1) *from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are given as follows: $s < n$ and*

1. *if $\nu(d_p) = \nu(d_q) > 0$, then $s = k_1 \mathrm{lcm}(d_p, d_q) + k_2 d_p + k_3 d_q$, $0 \le k_1 \le (p-1)(q-1)/\mathrm{lcm}(d_p, d_q)$, $0 \le k_2 \le (p-1)/d_p$, $0 \le k_3 \le (q-1)/d_q$;*
2. *if $\nu(d_p) > 0, \nu(d_q) > 0$ and $\nu(d_p) \ne \nu(d_q) > 0$, then $s = 2k_1 \mathrm{lcm}(d_p, d_q) + k_2 d_p + k_3 d_q$, $0 \le k_1 \le (p-1)(q-1)/(2\mathrm{lcm}(d_p, d_q))$, $0 \le k_2 \le (p-1)/d_p$, $0 \le k_3 \le (q-1)/d_q$;*
3. *if $\nu(d_p) > 0, \nu(d_q) = 0$, then $s = 2k_1 \mathrm{lcm}(d_p, d_q) + k_2 d_p + 2k_3 d_q$, $0 \le k_1 \le (p-1)(q-1)/(2\mathrm{lcm}(d_p, d_q))$, $0 \le k_2 \le (p-1)/d_p$, $0 \le k_3 \le (q-1)/(2d_q)$;*
4. *$\nu(d_p) = \nu(d_q) = 0$, then $s = 2k_1 \mathrm{lcm}(d_p, d_q) + 2k_2 d_p + 2k_3 d_q$, $0 \le k_1 \le (p-1)(q-1)/(2\mathrm{lcm}(d_p, d_q))$, $0 \le k_2 \le (p-1)/(2d_p)$, $0 \le k_3 \le (q-1)/(2d_q)$.*

Now the methods of constructing s-plateaued functions of the form (1) with prescribed s are obvious:

1. Among the self-reciprocal factors of $x^n + 1$ select some, whose degrees add up to s and form their product $h(x)$. We remark that s must be odd if n is odd, thus $x + 1$ must divide $h(x)$. If n is even then also s must be even, hence $h(x)$ will always be divisible by $(x+1)^g$ for some even integer $g \ge 2$.

2. Multiply $h(x)$ with a self-reciprocal polynomial of even degree, which is relatively prime to $(x^n + 1)/h(x)$. The resulting product $g(x)$ must be of degree at most $n - 1$.

3. Multiply $g(x)$ with x^{i_0}, where i_0 is the unique integer such that $A(x) = x^{i_0} g(x)$ is of the form (2). Note that $a_0 = 0$ for any $A(x)$, obtained this way.

4. The polynomial $f(x)$ of the form (1) corresponding to a $A(x)$ is then s-plateaued. Note that a_0 can be chosen as 0 or 1.

The following example leads to an easy proof of a result of [2].

Example 3. Construction of s-plateaued functions with maximal possible value for s:

As $n+s$ must be even, the maximal possible value for s is $s = n-2$. We have to choose a self-reciprocal divisor $h(x)$ of x^n+1 of degree $n-2$. The only possible choices for $h(x)$ are
(i) $h(x) = (x^n+1)/(x+1)^2$.
(ii) $h(x) = (x^n+1)/(x^2+x+1)$.
Now (i) implies that n is even and since then $(x+1)^2$ must divide $h(x)$, we need $4|n$, and (ii) implies that $3|n$. The step 2 in the above procedure can not be carried out, thus $g(x) = h(x)$, and $i_0 = 1$. We then get

$$A(x) = xh(x) = x + x^3 + x^5 + \cdots + x^{n-1} \quad \text{in case (i), and}$$
$$A(x) = xh(x) = x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots + x^{n-2} + x^{n-1} \quad \text{in case (ii).}$$

The following corollary easily follows from the argument used in the above example.

Corollary 3. *The quadratic function f of the form* (1) *is* $(n-2)$*-plateaued if and only if*

(i) $4|n$ *and* $f(x) = \mathrm{Tr_n}\left(\varepsilon x^2 + x^{2+1} + x^{2^3+1} + x^{2^5+1} + \cdots + x^{2^{n/2-1}+1}\right)$, $\varepsilon \in \{0,1\}$, *or*

(ii) $3|n$ *and* $f(x) = \mathrm{Tr_n}\left(\varepsilon x^2 + \sum_{i=1, i\not\equiv 0 \bmod 3}^{\lfloor n-1/2 \rfloor} x^{2^i+1}\right)$, $\varepsilon \in \{0,1\}$.

Compare our Corollary 3 with Theorem 2.4 in [2].

3 Conclusion

We enumerate quadratic s-plateaued functions from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_2$, given by (1). For squarefree integers $n = p_1 p_2 \cdots p_r$ we characterize the integers s, for which s-plateaued functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ of the form (1) exist. Methods for constructing such functions are also described. Our results generalize earlier work on the case $s = 1$, see [4, 5].

References

1. P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inform. Theory 51 (2005), 4286–4298.
2. R.W. Fitzgerald, Highly degenerate forms over finite fields of characteristic 2, Finite Fields Appl. 11 (2005), 165–181
3. R. A. Games and A. H. Chan, A fast algorithm for determining the complexity of a binary sequence with period 2^n, IEEE Trans. Inform. Theory 29 (1983) pp. 144–146.
4. K. Khoo, G. Gong, and D. R. Stinson, A new family of Gold-like sequences. In Proceedings of IEEE International Symposium of Information Theory (2002), p. 181.
5. K. Khoo, G. Gong, D. Stinson, A new characterization of semi-bent and bent functions on finite fields, Designs, Codes and Cryptography 38 (2006), 279–295.
6. G. Leander, G. McGuire, Construction of bent functions from near-bent functions, Journal of Combinatorial Theory, Series A 116 (2009), 960–970.
7. R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.