APN Functions in odd characteristic

Hans Dobbertin
University of Klagenfurt
Universitätstrasse 65–67
A-9020 Klagenfurt
Austria

Donald Mills
U.S. Army Research Labatory
Aberdeen Proving Ground
Aberdeen, MD 21005
USA

Eva Nuria Müller, Alexander Pott and Wolfgang Willems
Institute for Algebra and Geometry
Otto-von-Guericke-University Magdeburg
D-39016 Magdeburg

February 23, 2001

Abstract

Recently, the investigation of so-called almost perfect nonlinear (APN) functions has attracted a lot of research interest. In particular, the case of even characteristic has been investigated. The notion of "APN" has been extended to the non-binary case and several such mappings have been discovered. In this paper, we add some more examples. Our results explain some of the "open cases" in the tables of Helleseth, Rong and Sandberg [10].

1 Introduction

We assume that the reader is familiar with basic facts on finite fields; [12] is an excellent reference for those who need some help. The finite field with q elements is denoted by $\mathbb{F}_q$. Throughout this paper, q is a power of the prime p. We consider functions $f : \mathbb{F}_q \to \mathbb{F}_q$. Let $N_f(a,b)$ be the number of solutions $x \in \mathbb{F}_q$ of the equation

$$f(x+a) - f(x) = b, \quad a, b \in \mathbb{F}_q.$$

We are interested in functions f with the property that

$$\Delta_f := \max\{N_f(a,b) : a, b \in \mathbb{F}_q, a \neq 0\}$$

is "small". Obviously, $\sum_{a,b\in\mathbb{F}_q} N_f(a,b) = q^2$ and $\Delta_f \neq 0$. Since

$$N_f(0,b) = \begin{cases} 0 & \text{if } b \neq 0 \\ q & \text{if } b = 0 \end{cases} \tag{1}$$

we have

$$\sum_{\substack{a,b\in\mathbb{F}_q\\ a\neq 0}} N_f(a,b) = q^2 - q.$$

In fact, functions with the property $N_f(a,b)=1$ for all $a\neq 0$ are called *perfect nonlinear*, see Result 1.1. The term "nonlinear" is justified since linear functions f have $\Delta_f = q$, therefore a function f with $\Delta_f = 1$ is in some sense as nonlinear as possible.

It seems that the only functions f where it has been shown that Δ_f is small are power mappings $x \mapsto x^d$ with $d \leq q-1$ which we may assume without loss of generality. Even for this special class of functions the classification of all perfect nonlinear and almost perfect nonlinear functions is presently illusive. We also restrict ourselves to functions of this type. In this case, we sometimes write Δ_d and $N_d(a,b)$ instead of Δ_f and $N_f(a,b)$.

We say that two functions f and g have the same difference properties if the lists of values $N_f(a,b)$ and $N_g(a,b)$ with $a,b\in\mathbb{F}_q$ are equal. This motivates the definition of equivalent functions. The function $f(x^p)+ux+v$, $u,v\in\mathbb{F}_q$ has the same difference properties as $f(x)$. Functions $g(x)$ which can be obtained from $f(x)$ by a suitable composition of transformations of the type $f(x)\to f(x^p)+ux+v$ are called *equivalent.* Obviously, equivalent functions have the same difference properties. The linear term $ux+v$ shows that we may always assume $f(0)=0$ and $f(1)=1$ (which is trivially true for power mappings).

In the case of power mappings x^d, we may extend the notion of equivalence slightly: If $(d,q-1)=1$, the power mapping $x^{d^{-1}}$ has the same difference properties as x^d (d^{-1} calculated modulo $q-1$) since

$$\begin{aligned}
& (x+a)^d - x^d = b \\
\Leftrightarrow\quad & x+a = (x^d+b)^{d^{-1}} \\
\Leftrightarrow\quad & a = (x^d+b)^{d^{-1}} - (x^d)^{d^{-1}} \\
\Leftrightarrow\quad & a = (y+b)^{d^{-1}} - y^{d^{-1}} \quad \text{with } y = x^d.
\end{aligned}$$

Therefore, we also call the two power mappings x^d and $x^{d^{-1}}$ *equivalent.*

There is another interesting feature of power mappings, namely

$$N_d(1,a^d b) = N_d(a,b) \quad \text{for } a\neq 0. \tag{2}$$

This property follows from

$$\begin{aligned}
& (x+a)^d - x^d = b \\
\Leftrightarrow\quad & a^{-d}(y+1)^d - a^{-d}y = b, \quad y = a^d x \\
\Leftrightarrow\quad & (y+1)^d - y = a^d b \quad \text{with } y = a^d x
\end{aligned}$$

and it is in general not true for nonpower mappings.

Moreover, for APN functions the number of b's with $N_d(1,b)=2$ must be the same as the number of b's with $N_d(1,b)=0$: We have $\sum_{b\in\mathbb{F}_q} N_d(1,b) = q$ and the sum has exactly q terms in $\{0,1,2\}$.

Since we are interested in mappings with small Δ_f (sometimes called *low uniformity*), we begin with some remarks about the case $\Delta_f = 1$. Of course, this case is impossible in characteristic 2 since

$$f(x+a) - f(x) = b = f((x+a)+a) - f(x+a).$$

In odd characteristic, functions with $\Delta_f = 1$ are called *planar* or *perfect nonlinear* (PN). As far as the authors are aware, the only known planar power functions, up to equivalence, are those covered by the following result:

Result 1.1. *Let $f(x) = x^d$ be a mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ where $q = p^n$, p an odd prime. Then $\Delta_f = 1$ if*

- *$d = 2$;*
- *$d = p^k + 1$, where $n/\gcd(n,k)$ is odd;*
- *$d = (3^k + 1)/2$ where $p = 3$, k is odd and $\gcd(n,k) = 1$.*

The proofs for the first two parameters are fairly easy; the third case is more involved, see [4] and [11].

Planar functions are studied in geometry since they give rise to projective planes with certain transitivity properties. Dembowski and Ostrom [5] asked whether all planar functions f (up to equivalence) are of the form

$$f(x) = \sum_{i,j=0}^{n-1} a_{i,j} x^{p^i + p^j}.$$

The third series in Result 1.1 is an example of a planar function which is not of this type. It should also be mentioned that one example of a planar function is known which is not a power mapping, see [5]:

Result 1.2. *The function*

$$f(x) = x^{10} + x^6 - x^2$$

defined on $\mathbb{F}_{3^e}$ with $e = 2$ or e odd is a planar function.

Problem 1. *Find more planar functions, in particular more planar functions which are not power mappings.*

It seems that there is presently no chance to classify planar functions. It has been checked only for small fields that there are no more planar functions besides the known ones.

In the binary case planar functions cannot exist, as we mentioned already. This was one motivation to study almost perfect nonlinear functions: A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called *almost perfect nonlinear* if $\Delta_f = 2$. This is the best we can expect since $N_f(a,b)$ is even for $q = 2^n$. Therefore, the terminology "almost" is a little bit misleading for functions in characteristic 2: They should be called perfect nonlinear since they are (in the sense described above) as nonlinear as possible.

An investigation of the combinatorial objects corresponding to APN functions (similar to the correspondence between planar functions and projective planes) can be found in [3].

In the following result we summarize the present state of APN power mappings in even characteristic. We refer the reader to [6, 7, 8, 9].

Result 1.3. *Let $f(x) = x^d$ be a mapping $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then f is an APN function, i.e. $\Delta_d = 2$, if*

1. $d = 2^k + 1, \quad \gcd(n,k) = 1,$ *(Gold case);*
2. $d = 2^{2k} - 2^k + 1, \quad \gcd(n,k) = 1,$ *(Kasami case);*
3. $d = 2^n - 2 \equiv -1 \bmod 2^n - 1, \quad n$ *odd, (Kloosterman case);*
4. $d = 2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1, \quad n = 5k;$
5. $d = 2^{k/2} + 3, \quad n = 2k + 1$ *odd, (Welch case);*
6. $d = 2^{2k} + 2^k - 1, \quad 4k + 1 \equiv 0 \bmod n,$ *(Niho case).*

Problem 2. *Prove or disprove that this list, up to equivalence, is complete for APN power mappings. Try to find APN functions which are not power mappings.*

We note an interesting difference between the first two cases and the remaining four instances in Result 1.3. In the Gold and the Kasami case, for a given n we have several choices for k which give APN functions. In cases (3)–(6), there is always just one APN function for each n.

It is worth mentioning a slightly different concept called maximum nonlinearity: A function is called *maximum nonlinear* if its so called *Walsh spectrum* has a certain extremal property, see [2]. If n is odd, this type of nonlinearity implies the APN property. With the exception of cases (3) and (5) in Result 1.3, all APN functions with n odd are in fact maximum nonlinear.

In this paper, we will investigate APN power mappings in fields of odd characteristic.

2 Missing entries in the Helleseth-Rong-Sandberg tables

The paper [10] contains tables of integers d such that x^d is APN in $\mathbb{F}_{p^n}$, where $p^n \in \{2^2, 2^3, \ldots, 2^{11}, 3^2, 3^3, \ldots 3^7, 5^2, \ldots, 5^5, 7^2, 7^3, 7^4, 11^2, 11^3\}$. The authors did a computer search showing that their lists are complete (up to equivalence). Their paper contains many theorems showing that certain integers d yield APN functions. In the binary case, by now all the entries can be explained by a Theorem (see Result 1.3). In other words, all the values d which give rise to an

Table 1: APN power mappings which are not yet "explained".

	q	d
I	3^5	134
II	3^5	152
III	3^7	40
IV	3^7	224
V	3^7	274
VI	5^3	14
VII	5^5	843

APN function are members of an infinite family of APN functions. However, in the nonbinary situation, some values cannot be explained yet (Table 1).

In this paper, we prove the following Theorems:

Theorem 2.1. *In $\mathbb{F}_{3^n}$ $(n > 3)$ the power mapping x^d satisfies $\Delta_d \leq 2$ for*

$$d = \begin{cases} \dfrac{3^{(n+1)/2} - 1}{2} & \text{if } n \equiv 3 \mod 4 \\ \dfrac{3^{(n+1)/2} - 1}{2} + \dfrac{3^n - 1}{2} & \text{if } n \equiv 1 \mod 4. \end{cases}$$

This theorem explains the cases I and III, except that we are not yet able to show $\Delta_d = 2$.

Theorem 2.2. *In $\mathbb{F}_{3^n}$ the power mapping x^d satisfies $\Delta_d \leq 2$ for*

$$d = \begin{cases} \dfrac{3^{n+1} - 1}{8} & \text{if } n \equiv 3 \mod 4 \\ \dfrac{3^{n+1} - 1}{8} + \dfrac{3^n - 1}{2} & \text{if } n \equiv 1 \mod 4. \end{cases}$$

This explains cases II and V if we can show $\Delta_d = 2$. Regarding $p = 5$, we have the following conjecture explaining VII:

Problem 3. *Show that $\Delta_d = 2$ in Theorems 2.1and 2.2.*

Conjecture 1. *In $\mathbb{F}_{5^n}$ the power mapping x^d is an APN function for*

$$d = \frac{5^n - 1}{4} + \frac{5^{(n+1)/2} - 1}{2}.$$

We do not know how the cases IV and VI may fit into an infinite series.

3 Preliminaries

Following the notation in [10], we define

$$u_x := x^d, \quad u_{x+1} := (x+1)^d. \tag{3}$$

Because of (2), it suffices to show

$$N_d(1,b) \leq 2$$

for all $b \in \mathbb{F}_q$ (with equality for at least one pair (a,b)) in order to prove that x^d is APN. In other words, we have to calculate the number of solutions $x \in \mathbb{F}_q$ with

$$(x+1)^d - x^d = b, \tag{4}$$

i.e. $u_{x+1} - u_x = b$.

We need some more prerequisites before we can start proving Theorems 2.1 and 2.2. Let q be an odd prime power. The mapping

$$\begin{array}{rccc} \chi: & \mathbb{F}_q^* & \to & \{-1,+1\} \\ & x & \mapsto & x^{(q-1)/2} \end{array}$$

is called the *quadratic character*. It maps the squares in $\mathbb{F}_q^*$ (the multiplicative group $\mathbb{F}_q \setminus \{0\}$) to 1 and the nonsquares to -1. It is a homomorphism from the multiplicative group of the field into the group with just two elements ± 1. Sometimes we extend χ by setting $\chi(0) = 0$ to a mapping $\mathbb{F}_q \mapsto \{-1,0,1\}$.

The following lemma will be crucial in the proofs of the main theorems.

Lemma 3.1. *In $\mathbb{F}_{3^n}$, n odd, we define*

$$Q := \{x^2 : x \in \mathbb{F}_{3^n}\}$$

and

$$M_a := \{x^d + (x+a)^d : x, x+a \in Q\},$$

where $d = 3^{(n+1)/2}+1$ or $d = 4$. Then

$$M_a \cap (-M_a) = \emptyset$$

for all $a \in \mathbb{F}_{3^n}^*$.

Proof. Note that -1 is a nonsquare since n is odd. Therefore, an element $a \in \mathbb{F}_{3^n}$, $a \neq 0$, is either a square or $-a$ is a square. Since $M_a = M_{-a}$, we may assume that a is a square. Then

$$x^d + (x+a)^d = a^d \left(\left(\frac{x}{a}\right)^d + \left(\left(\frac{x}{a}\right)^d + 1 \right) \right)$$

shows that it is sufficient to prove the lemma for the case $a = 1$.

Suppose that $M_1 \cap (-M_1) \neq \emptyset$, say $x, x+1, u, u+1$ are squares which satisfy

$$x^d + (x+1)^d = -(u^d + (u+1)^d). \tag{5}$$

Case A: $d = 3^{\frac{n+1}{2}} + 1$. Put $m = \frac{n+1}{2}$, $y = x^{3^m}$ and $v = u^{3^m}$. Then (5) becomes

$$xy + (x+1)(y+1) = -uv - (u+1)(v+1)$$

or, equivalently,

$$2xy + x + y + 1 = -(2uv + u + v + 1). \tag{6}$$

We raise both sides of (6) to the 3^m-th power which means that we replace x by y, u by v, y by x^3 and v by u^3; this leads to

$$x^3y - x^3 - y - 1 = -(u^3v - u^3 - v - 1). \tag{7}$$

Adding (6) and (7) we get

$$x(x+1)(x-1)(y-1) = -u(u+1)(u-1)(v-1). \tag{8}$$

Note that $x(x+1)(x-1)(x^{3^m} - 1) = 0$ if and only if $x \in \mathbb{F}_3$. Therefore we have

$$u \in \mathbb{F}_3 \quad \Leftrightarrow \quad x \in \mathbb{F}_3.$$

However, our lemma holds trivially for $\mathbb{F}_3$. Therefore the elements x and u which define the elements in the intersection $M_1 \cap -M_1$ (see (5)) cannot be elements of $\mathbb{F}_3$ (observe that $M_1 = \{1\} \subset \mathbb{F}_3$). From now on we may assume that both sides of (8) are $\neq 0$. We obtain

$$\begin{aligned} -1 &= \frac{x(x+1)(x-1)(y-1)}{u(u+1)(u-1)(v-1)} \\ &= \frac{x(x+1)(x-1)(x-1)^{3^m}}{u(u+1)(u-1)(u-1)^{3^m}} \\ &= \frac{x(x+1)}{u(u+1)} \times \left(\frac{x-1}{u-1}\right)^d. \end{aligned}$$

Since $x, x+1, u, u+1$ are squares and d is even, the expression on the right hand side is a square, however -1 is a nonsquare in $\mathbb{F}_{3^n}$.

Case B: $d = 4$. This case is actually easier. We consider

$$(u+1)^4 + u^4 + (x+1)^4 + x^4 = 2u^4 + u^3 + u + 2x^4 + x^3 + x + 2 = 0$$

which is equivalent to

$$(u^2 + u + x^2 + x + 1)^2 + (u^2 + u)(x^2 + x) = 0.$$

Note that we do all the computations in a field of characteristic 3. Since $u^2 + u$ and $x^2 + x$ are both squares and -1 is not a square, this equation is solvable only for $u(u+1) = 0$ and $x = 1$ (or vice versa $x \leftrightarrow u$). However, $x+1$ is not a square, hence this case does not satisfy the assumptions of our lemma. $\square$

A polynomial $f \in \mathbb{F}_{q^n}[x]$ is called *q-linearized* if

$$\begin{array}{rrcl} & f(x+y) & = & f(x)+f(y) \\ \text{and} & f(x\lambda) & = & f(x)\lambda \end{array}$$

holds for all $x, y \in \mathbb{F}_{q^n}$ and $\lambda \in \mathbb{F}_q$. In other words: The polynomial mapping $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ corresponding to a q-linearized f is a linear $\mathbb{F}_q$-mapping. The reader is referred to [12] for more background on linearized polynomials. It is easy to see that polynomials of the form

$$f = \sum_{i=0}^{n-1} a_i x^{q^i}$$

are linearized and, conversely, all linearized polynomials are of this form.

In this paper, we will meet several linearized polynomials of the form

$$x^{q^m} + bx$$

and it will be important to decide for which b these polynomials describe bijective linear mappings.

Lemma 3.2. *The polynomial $x^{q^m} + bx \in \mathbb{F}_{q^n}[x]$ describes a bijective linear mapping if and only if $-b$ is not a $(q^m - 1)$-th power in $\mathbb{F}_{q^n}$.*

Proof. The mapping $x \mapsto x^{q^m} + bx$ is bijective if and only if the equivalence

$$x^{q^m} + bx = 0 \quad \Leftrightarrow \quad x = 0$$

holds. □

We note that the problem whether -1 is a t-th power can be easily decided: The t-th powers in $\mathbb{F}_{q^n}^*$ form a subgroup H of order $(q^n - 1)/\gcd(t, q^n - 1)$. We have $-1 \in H$ if and only if $|H|$ is even. Together with the well known formula

$$\gcd(z^n - 1, z^m - 1) = z^{\gcd(n,m)} - 1, \quad z \in \mathbb{Z} \tag{9}$$

we obtain the following characterization:

Corollary 3.3. *Let q be an odd prime power. The polynomial mapping $x^{q^m} + x$ is a bijection if and only if $n/\gcd(n, m)$ is odd.*

Proof. Use (9) and the fact that $(q^{st} - 1)/(q^s - 1) \equiv t \bmod 2$ for odd integers q. □

4 APN functions for $p = 3$

In this section we give proofs for the two main Theorems 2.1 and 2.2.

Proof of Theorem 2.1. We check $N_d(1, b) \leq 2$ for all $b \in \mathbb{F}_{3^n}$ where $n \equiv 3 \bmod 4$ and $d = (3^{(n+1)/2} - 1)/2$. This also implies $N_d(1, b) \leq 2$ for the other value of

d in the case $n \equiv 1 \bmod 4$: Simply replace n by $3n \equiv 3 \bmod 4$, then x^e with $e = (3^{(3n+1)/2} - 1)/2$ is an APN function in $\mathbb{F}_{3^{3n}}$ (if we have proved Theorem 2.1 for the case $\equiv 1 \bmod 4$). Therefore, the equation $(x+1)^e - x^e = b$ has at most two solutions in $\mathbb{F}_{3^{3n}}$. But

$$x^{(3^{(3n+1)/2}-1)/2} = x^{(3^{(n+1)/2}-1)/2+(3^n-1)/2}$$

since

$$\begin{aligned} e = \frac{3^{(3n+1)/2}-1}{2} &= \frac{(3^n-1)\cdot 3^{(n+1)/2} + (3^{(n+1)/2}-1)}{2} \\ &\equiv \frac{3^n-1}{2} + \frac{3^{(n+1)/2}-1}{2} \qquad \bmod (3^n-1). \end{aligned}$$

Note that $x^d = x^{d'}$ in $\mathbb{F}_{3^n}$ if and only if $d \equiv d' \bmod (3^n - 1)$.

From now on let $m = (n+1)/2$. We consider $u_x + b = u_{x+1}$ (see (3) for the definition of u_x) which implies

$$(u_x + b)^{3^m+1} = (u_{x+1})^{3^m+1}. \tag{10}$$

Rewriting (10) yields

$$u_x^{3^m} u_x + u_x^{3^m} b + b^{3^m} u_x + b^{3^m} b = u_{x+1}^{3^m} u_{x+1}. \tag{11}$$

Since

$$(3^m+1)\cdot \underbrace{\frac{3^m-1}{2}}_{d} = 3^n + \frac{3^n-1}{2}, \tag{12}$$

we have

$$u_x^{3^m+1} = (x^d)^{3^m+1} = x^{(3^n-1)/2}\cdot x = \chi(x)\cdot x \tag{13}$$

and we may reformulate (11):

$$\chi(x)\cdot x + u_x^{3^m} b + b^{3^m} u_x + b^{3^m+1} = \chi(x+1)\cdot(x+1).$$

This is equivalent to

$$\chi(x)\cdot x - \chi(x+1)\cdot(x+1) = 2b^{3^m+1} + 2b^{3^m} u_x + 2u_x^{3^m} b. \tag{14}$$

Case A: $\chi(x) = \chi(x+1)$ or $x = 0$ or $x = 2$. In this case, we have $\chi(x)\cdot x - \chi(x+1)\cdot(x+1) = \pm 1$. We determine the number of solutions in x that satisfy at least one of the two equations

$$\epsilon + b^{3^m+1} = 2b^{3^m} u_x + 2u_x^{3^m} b, \quad \epsilon = \pm 1. \tag{15}$$

We have

$$\epsilon = \begin{cases} +1 & \text{if } \chi(x) = \chi(x+1) = -1 \text{ or } x = 2 \\ -1 & \text{if } \chi(x) = \chi(x+1) = 1 \text{ or } x = 0. \end{cases}$$

To be more precise, let

$$A_1(b) := \{x \in F_{3^n} : 1 + b^{3^m+1} = 2b^{3^m} u_x + 2u_x^{3^m} b,$$
$$\chi(x)\chi(x+1) = -1 \text{ or } x = 2\}$$

and

$$A_2(b) := \{x \in F_{3^n} : -1 + b^{3^m+1} = 2b^{3^m} u_x + 2u_x^{3^m} b,$$
$$\chi(x) = \chi(x+1) = 1 \text{ or } x = 0\}.$$

We will show $|A_1(b) \cup A_2(b)| \leq 1$.

The polynomial on the right hand side of (15) is linearized in u_x, hence it describes a linear mapping $\mathbb{F}_{3^n} \to \mathbb{F}_{3^n}$ where $\mathbb{F}_{3^n}$ is considered as a vector space over $\mathbb{F}_3$. We are now going to show that this mapping is injective and hence bijective (in case $b \neq 0$). Bijectivity of

$$b^{3^m} u_x + u_x^{3^m} b = 0$$

is equivalent to the property that $-b^{3^m-1}$ is not a $(3^m - 1)$-th power of an element in $\mathbb{F}_{3^n}$, see Lemma 3.2. But this is true since -1 is not a square. This shows that we have, for a given b, at most one solution u_x for the two equations (15). Since $\gcd(d, 3^n - 1) = 2$ (see (12)), there are at most two solutions with $x^d = u_x$, which just differ by the sign. Therefore only one of the two solutions can be a square (or a nonsquare) and we have shown $|A_1(b)|, |A_2(b)| \leq 1$. We are now going to show that, given b, not both of the equations in (15) can have solutions. Assume that u_x is a solution with $x \in A_1(b)$, i.e. $\epsilon = 1$ and u_y is a solution with $y \in A_2(b)$, hence $\epsilon = -1$. We add the two equations and obtain

$$0 = b^{3^m+1} + 2b^{3^m}(u_x + u_y) + 2(u_x + u_y)^{3^m} b.$$

As before (linearized polynomial in $u_x + u_y$) we see that we have at most one solution $u_x + u_y = 2b$. This shows

$$u_{x+1} = u_x + b = -u_y,$$

where u_{x+1} is a square, but $-u_y$ is a nonsquare if $u_y \neq 0$. This implies $u_{x+1} = u_y = 0$, hence $x = 2$ and $y = 0$. But it is easy to check that $2 \in A_1(b)$ and $0 \in A_2(b)$ is impossible. Note that $u_0 = 0$ and $u_2 = 1$.

Case B: $\chi(x) = -\chi(x+1)$. In this case, the left hand side of (14) is $\pm(x-1)$. Using (13), we have to find the number of solutions of the equations

$$2u_x^{3^m+1} + \epsilon = 2b^{3^m+1} + 2b^{3^m} u_x + 2u_x^{3^m} b, \quad \epsilon = \pm 1,$$

where $\epsilon = +1$ if $\chi(x) = 1$, otherwise $\epsilon = -1$. We put

$$A_3(b) := \{x \in \mathbb{F}_{3^n} : 2u_x^{3^m+1} + 1 = 2b^{3^m+1} + 2b^{3^m} u_x + 2u_x^{3^m} b,$$
$$\chi(x) = 1, \chi(x+1) = -1\}$$

and

$$A_4(b) := \{x \in \mathbb{F}_{3^n} : 2u_x^{3^m+1} - 1 = 2b^{3^m+1} + 2b^{3^m}u_x + 2u_x^{3^m}b,$$
$$\chi(x) = -1, \chi(x+1) = +1\}$$

and have to show that $|A_3(b) \cup A_4(b)| \leq 1$ for all b. We replace u_x by $u+b$ and obtain

$$2(u+b)^{3^m}(u+b) + \epsilon = 2b^{3^m+1} + 2b^{3^m}u + 2b^{3^m+1} + 2(u+b)^{3^m}b, \quad \epsilon = \pm 1$$

which yields

$$2u^{3^m+1} + \epsilon = b^{3^m+1}. \tag{16}$$

Since $\gcd(3^m+1, 3^n-1) = 2$ (see (12)), given ϵ and b there are at most two solutions of (16) for u. Therefore, given b, we have at most four elements x in $A_3(b) \cup A_4(b)$ such that $u_x - b = \pm\sqrt{c_\epsilon}$, hence $u_x = \pm\sqrt{c_\epsilon} + b$ and $u_{x+1} = u_x + b = \pm\sqrt{c_\epsilon} + 2b = -(\mp\sqrt{c_\epsilon} + b)$. Since u_x and u_{x+1} both are squares (d is even!) and -1 is a nonsquare in $\mathbb{F}_{3^n}$, it is impossible to get suitable solutions for both square roots of c_ϵ.

We are now going to show that there is at most <u>one</u> solution of $(x+1)^d - x^d = b$ with $\chi(x) = -\chi(x+1)$. Assume there is a solution x with $\chi(x) = 1$ and $\chi(x+1) = -1$. Then

$$-1 = \chi(x) \cdot x + \chi(x+1) \cdot (x+1) = u_x^{3^m+1} + u_{x+1}^{3^m+1}.$$

Another solution y with $\chi(y) = -1$ and $\chi(y+1) = 1$ yields

$$u_y^{3^m+1} + u_{y+1}^{3^m+1} = 1.$$

Since $u_x, u_{x+1}, u_y, u_{y+1}$ are all squares, we have solutions in u of the two equations

$$u^{3^m+1} + (u+b)^{3^m+1} = \epsilon$$

with $\epsilon = \pm 1$, u and $u+b$ both squares. This is impossible due to Lemma 3.1.

Proof of Theorem 2.2. As in Theorem 2.1 it is sufficient to consider the case $n \equiv 3 \bmod 4$, otherwise replace n by $3n$ and consider the difference properties for the exponent $3^{3n+1} - 1)/8$ in the subfield $\mathbb{F}_{3^n}$ of $\mathbb{F}_{3^{3n}}$. So let us assume $n \equiv 3 \bmod 4$, i.e. $d = (3^{n+1} - 1)/8$. In particular, d is even. Again, -1 is a nonsquare in $\mathbb{F}_{3^n}$. With the notation as in the proof of Theorem 2.1, we get

$$\chi(x) \cdot x = u_x^4$$

where χ is again the quadratic character, i.e. $\chi(x) = x^{(3^n-1)/2}$, and $u_x = x^d$, see (3). Note that

$$\frac{3^n - 1}{2} + 1 \equiv \frac{3^{n+1} - 1}{2} \mod (3^n - 1).$$

Again, we shall prove that $N_d(1, b) \leq 2$ for all $b \in \mathbb{F}_{3^n}$. We look at the fourth power of the equation $u_{x+1} = u_x + b$ which yields

$$\chi(x+1) \cdot (x+1) = u_x^4 + bu_x^3 + b^3 u_x + b^4 = \chi(x) \cdot x + bu_x^3 + b^3 u_x + b^4$$

(note that the characteristic of the underlying field is 3). Therefore,

$$[\chi(x+1) - \chi(x)] \cdot x + \chi(x+1) = b^4 + b^3 u_x + bu_x^3. \tag{17}$$

Lemma 3.2 shows that the mapping

$$u_x \mapsto b^3 u_x + bu_x^3 \tag{18}$$

is a bijective linear mapping since -1 is a nonsquare.

To investigate (17), we distinguish two cases.

Case A: $\chi(x) = \chi(x+1)$ or $x = 0$ or $x = 2$. In this case, we have

$$\epsilon = b^4 + b^3 u_x + bu_x^3, \quad \epsilon = \pm 1 \tag{19}$$

where $\epsilon = \chi(x)$ if $x \neq 0$ and $\epsilon = 1$ if $x = 0$. Given ϵ and b, there is at most one u_x which satisfies (19) in view of (18). It might also be possible that there are solutions x and y of (18) with

$$\begin{aligned} b^4 + b^3 u_x + bu_x^3 &= 1 \\ b^4 + b^3 u_y + bu_y^3 &= -1 \end{aligned}$$

where $\chi(x) = 1$ and $\chi(y) = -1$ or $y = 0$. In this situation, we obtain the following expression by adding the two equations:

$$0 = 2b^4 + b^3(u_x + u_y) + b(u_x + u_y)^3.$$

The only solution is $u_x + u_y = 2b$ (note again the bijectivity of (18)), hence $x^d + y^d = 2b$. But then $(x+1)^d = x^d + b = -y^d$ which is impossible since $(x+1)^d$ is a square, but $-y^d$ is a nonsquare or $y = 0$.

Case B: $\chi(x) \neq \chi(x+1)$. We get

$$\chi(x)(x-1) = b^4 + b^3 u_x + bu_x^3$$

where $\epsilon = \chi(x)$. We replace u_x by $u + b$ and obtain

$$(u+b)^4 - \epsilon = b^4 + b^3(u+b) + b(u+b)^3$$

which gives

$$u^4 = 2b^4 + \epsilon.$$

There are two possible solutions for u (note that the order $3^n - 1$ of the multiplicative group of the field is divisible by 2 and not by 4 since n is odd). If c is one solution, then the other solution is $-c$ and we get

$$\begin{aligned}
u_x^{(1)} &= c+b \\
u_{x+1}^{(1)} &= c+2b = c-b \\
u_x^{(2)} &= -c+b = -u_{x+1}^{(1)} \\
u_{x+1}^{(2)} &= -c+2b = -c-b = -u_x^{(1)}
\end{aligned}$$

Since d is even (using the value of n modulo 4), both u_x and u_{x+1} have to be squares, therefore at most one of the two solutions represents a solution of

$$(x+1)^d - x^d = b.$$

However, it might be possible that there are simultaneous solutions for $\epsilon = 1$ and $\epsilon = -1$:

$$(x+1)^d - x^d = (y+1)^d - y^d = b$$

where

$$\chi(x) = 1 = \chi(y+1), \quad \chi(y) = -1 = \chi(x+1).$$

In this case, we would obtain

$$\begin{aligned}
u_{x+1}^4 = (u_x+b)^4 &= \chi(x+1)(x+1) \\
&= -\chi(x)x + \chi(x+1) \\
&= -u_x^4 + \chi(x+1)
\end{aligned}$$

and

$$u_{y+1}^4 = (u_y+b)^4 = -u_y^4 + \chi(y+1).$$

Since u_x, u_x+b, u_y, u_y+b are all squares, this contradicts Lemma 3.1.

5 Power functions with low uniformity

In this final section we collect some results on low uniformity power mappings. We begin with an easy observation also contained in [10]:

Lemma 5.1. *If d is not a power of p (the characteristic of $\mathbb{F}_q$), then the power mapping x^d in $\mathbb{F}_q$ satisfies $N_d(a,b) \le d-1$ for all $a, b \in \mathbb{F}_q$, $a \neq 0$.*

Proof. The number of solutions of $(x+a)^d - x^d = b$ is obviously bounded by $d-1$ as $(x+a)^d - x^d - b$ is not the zero polynomial. □

Note that $(x+a)^d - x^d = a^d$ if d is a power of p, hence the observation cannot hold for powers of p.

Using 5.1 it seems reasonable to look at "small" d's in order to get low uniformity. We know already $\Delta_2 = 1$ ($p \neq 2$, see Result 1.1) and $\Delta_3 = 2$ ($p \neq 3$, see 5.1 and Theorem 3 in [10]); the next case is $d = 4$:

Theorem 5.2. *Let p be an odd prime. Then*

$$\Delta_4 = \begin{cases} 1 & \textit{if } n \textit{ is odd and } p = 3 \\ 2 & \textit{if } n = 1 \textit{ and } p = 7 \\ 3 & \textit{otherwise.} \end{cases}$$

Proof. Clearly $\Delta_4 \leq 3$ by Lemma 5.1. If $p = 3$ and n is odd, we have $\Delta_4 = 1$ in view of Result 1.1. We get

$$(x+1)^4 - x^4 = b \quad \Leftrightarrow \quad 4x^3 + 6x^2 + 4x + (1-b) = 0. \tag{20}$$

In order to show that $\Delta_4 = 3$ we must check that (20) has three solutions for some value of b. We choose $b = 1$, hence we consider

$$x(4x^2 + 6x + 4) = 0.$$

The discriminant of the quadratic is -28, therefore $4x^2+6x+4$ has two different solutions $\neq 0$ in $\mathbb{F}_{p^2} (\leq \mathbb{F}_{p^n})$. If n is even, $\mathbb{F}_{p^2} \leq \mathbb{F}_{p^n}$ and the two solutions are also contained in $\mathbb{F}_{p^n}$. For $p = 7$, we have

$$x^3 + 5x^2 + x + 2(1-b) = 0.$$

Taking $b = 2$, we get $x^3 + 5x^2 + x + 5 = (x+5)(x^2+1)$ where $x^2 + 1$ has two roots in $\mathbb{F}_{49} \setminus \mathbb{F}_7$. This shows $N_4(1,2) = 3$ in the case $p = 7$ and the proof is complete. It is easy to check that $\Delta_4 = 2$ for $p = 7$ and $n = 1$.

Now let us assume $p \neq 2, 3$ and $p^n \neq 7$. We have to show that (20) has exactly three solutions for an appropriate b. Replace x by $x - \frac{1}{2}$ and multiply by 8 to get

$$8x^3 + 2x + c = 0,$$

hence

$$y^3 + y + c = 0 \tag{21}$$

(note that the constant term is irrelevant at this point). Assume that γ is a root of (21), i.e. $c = -\gamma^3 - \gamma$. We get

$$(y^2 + y\gamma + \gamma^2 + 1)(y - \gamma) = 0.$$

The discriminant of the quadratic is $-3\gamma^2 - 1$. It is routine to check that γ is a root of $y^2 + y\gamma + \gamma^2 + 1$ if and only if $-3\gamma^2 - 1 \neq 0$ (in which case $y^3 + y + c = (y-\gamma)^3$). In order to show that we can choose γ such that (21) has three different solutions we need an argument that there is at least one square $-3\gamma^2 - 1$ in $\mathbb{F}_{p^n}$ (note that this is not the case if $p^n = 7$). This follows from the fact that the set of squares in $\mathbb{F}_q$ form a difference set if $q \equiv 3 \bmod 4$ and a partial difference set if $q \equiv 1 \bmod 4$. The same holds for the nonsquares. We refer the reader to [1] for the necessary background on difference sets. As a consequence, we get

$$|\{a\gamma^2 + b\}| \in \left\{ \frac{q-3}{4}, \frac{q-1}{4}, \frac{q-5}{4} \right\}$$

for $a \neq 0$ which shows that we have enough choices for γ to ensure that $y^3 + y - \gamma^3 - \gamma$ has three distinct roots. $\square$

Another interesting case is $d = -1$, i.e. the power mapping $x \mapsto x^{-1}$ in $\mathbb{F}_q$. We must be a little bit careful since 0^{-1} is undefined. Therefore, we consider $d = q - 2$. The power mapping $x \to x^{q-2}$ fixes 0 and it is the multiplicative inversion for the elements $\neq 0$. Here is what we know:

Theorem 5.3. *Let $d = q - 2$ and $q = p^n$. Then the power mapping x^d in $\mathbb{F}_q$ with $q > 2$ satisfies*

$$\Delta_d = \begin{cases} 2 & \text{if } p^n \equiv 2 \text{ mod } 3 \\ 3 & \text{if } p = 3 \\ 4 & \text{if } p^n \equiv 1 \text{ mod } 3. \end{cases}$$

Proof. [10] The fundamental equation $(x+1)^d - x^d = b$ is for $x \neq 0, -1$ equivalent to $(x+1)^{-1} - x^{-1} = b$, hence equivalent to

$$bx^2 + bx + 1 = 0.$$

This equation has at most two solutions. The cases $x = 0$ and $x = -1$ are solutions of $(x+1)^d - x^d = 1$, hence we just have to consider the polynomial $x^2 + x + 1 = (x^3 - 1)/(x - 1)$. This polynomial has two solutions if $p^n \equiv 1$ mod 3, one solution if $p = 3$ and no solutions in the remaining case. □

There is another family of 3-uniform mappings which follow from the results in [10]:

Theorem 5.4 (Theorem 11 and Corollary 1 in [10]). *The power mapping x^d with $d = \frac{7^k+1}{2}$ in $\mathbb{F}_{7^n}$, n even and $\gcd(2n, k) = 1$ satisfies $\Delta_d = 3$.*

In the final two theorems we discuss new exponents with low uniformity. The first series lives in fields $\mathbb{F}_{p^n}$, n odd and $p \equiv 1$ mod 4, in the second case the field has characteristic 3.

Theorem 5.5. *Let n be odd and p be a prime $\equiv 1$ mod 4. Then $\Delta_d \leq 3$ holds for the power mapping with exponent $d = \frac{p^n-1}{2} + p + 1$ in the field $\mathbb{F}_{p^n}$. Moreover, $\Delta_d = 3$ if $d \equiv 0$ mod 4.*

Proof. As usual, we consider the basic equation $(x+1)^d - x^d = b$, equivalently

$$\chi(x+1) \cdot (x^p + 1)(x+1) - \chi(x) \cdot x^{p+1} = b \tag{22}$$

where χ is the quadratic character on $\mathbb{F}_{p^n}$.

Case A: $x = 0$ or $x = -1$. Note that $x = 0$ is a solution only for $b = 1$, whereas $x = -1$ is a solution for $b = -1$ (note that d is even).

Case B: $\chi(x) = \chi(x+1)$. In this situation, equation (22) yields

$$x^p + x = \chi(x) \cdot b - 1. \tag{23}$$

Since the mapping $x \mapsto x + x^p$ is a bijective linear mapping (see Lemma 3.2), the equation (23) has at most one solution for given b and $\chi(x)$. However, it is impossible that there is a square u and a nonsquare v which satisfy

$$\begin{aligned} u^p + u &= -1 + b \\ v^p + v &= -1 - b \end{aligned} \tag{24}$$

such that $\chi(u) = \chi(u+1) = 1$ and $\chi(v) = \chi(v+1) = -1$. Just add the two equations in (24) to obtain

$$(u+v)^p + (u+v) = -2.$$

This equation has the unique solution $u + v = -1$, i.e. $u = -(1+v)$. Since -1 is a square this is impossible. We also note that, given b, there are no simultaneous solutions for Case A and Case B. Thus, for a given b we found at most one solution so far.

Case C: $\chi(x) = -\chi(x+1)$. We assume $\chi(x) = -1$. From (22) we obtain

$$2x^{p+1} + x^p + x = b - 1. \tag{25}$$

Replace x by $(y-1)/2$ to get

$$y^{p+1} = 2b + 2 \tag{26}$$

Since $p+1$ is even, (26) can be written as

$$\hat{y}^2 = 2b + 2, \quad \text{where} \quad \hat{y} = y^{(p+1)/2}. \tag{27}$$

Note that $p \equiv 1 \bmod 4$ and thus $\gcd((p+1)/2, p^n - 1) = 1$, so the power mapping $x \mapsto x^{(p+1)/2}$ is a bijection on $\mathbb{F}_{p^n}$. The quadratic equation (27) has (at most) two solutions for y, say $\pm A$, the corresponding solutions of (25) are

$$x_{\pm} = \frac{\pm A - 1}{2},$$

where $A \in \mathbb{F}_{p^n}$. We have

$$x_{\pm} + 1 = -x_{\mp}.$$

This shows that at most one of the two solutions satisfies the assumptions $\chi(x_{\pm}) = -1$ and $\chi(x_{\pm}+1) = 1$, since $1 = \chi(x_{\pm}+1) = \chi(-(x_{\mp})) = \chi(x_{\mp})$ (note that -1 is a square!).

Finally we must check $\Delta_d = 3$ for $d \equiv 0 \bmod 4$: We take $b = 0$, in which case we have the three solutions of $(x+1)^d - x^d = 0$

$$x_1 = \frac{-1}{2}, \quad x_{2/3} = \frac{-1 \pm \sqrt{-1}}{2}$$

which are all distinct. □

Theorem 5.6. *Let $n \equiv 2 \bmod 4$, $n > 2$. The power mapping x^d in $\mathbb{F}_{3^n}$ with exponent $d = \frac{3^n-1}{2} + 3^{(n-2)/2} + 1$ satisfies $\Delta_d \leq 3$.*

Proof. The fundamental equation $(x+1)^d - x^d = b$ becomes

$$\chi(x+1) \cdot (x+1)^{3^{(n-2)/2}+1} - \chi(x) \cdot x^{3^{(n-2)/2}+1} = b$$

where $\chi(x) = x^{(3^n-1)/2}$ is the quadratic character on $\mathbb{F}_{3^n}$. As usual, we have to consider the cases $x = 0, -1$, $\chi(x) = \chi(x+1)$ and $\chi(x) = -\chi(x+1)$. The case

$x = 0, -1$ gives solutions with $b = 1$ and $b = -1$. If $\chi(x) = \chi(x+1)$ we get the linearized equations
$$x^{3^{(n-2)/2}} + x + 1 = \chi(x) \cdot b.$$
Since $n/\gcd(n, (n-2)/2)$ is odd, these equations have, given b, exactly one solution (see Corollary 3.3). Adding two hypothetical solutions u with $\chi(u) = \chi(u+1) = 1$ and v with $\chi(v) = \chi(v+1) = -1$ corresponding to the same b, we obtain
$$(u+v)^{3^{(n-2)/2}} + (u+v) = 1,$$
which has the unique solution $(u+v) = -1$. Since -1 is a square we obtain a contradiction $u = -(1+v)$ as in the proof of Theorem 5.5.

Now let us assume $\chi(x) = -1$ and $\chi(x+1) = 1$, the other case $\chi(x) = 1 = -\chi(x+1)$ is analogous. Our equation reduces to
$$2x^{3^{(n-2)/2}+1} + x^{3^{(n-2)/2}} + x = b - 1.$$
Substituting $y + 1$ instead of x gives
$$y^{3^{(n-2)/2}+1} = \left[y^{\frac{3^{(n-2)/2}+1}{2}}\right]^2 = 2(b+2).$$
We can finish this case as in the proof of Theorem 5.5.

$\square$

References

[1] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 2 ed., 1999.

[2] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, in Advances in Cryptology – EUROCRYPT 94, A. D. Santis, ed., vol. 950 of Lecture Notes in Computer Science, New York, 1995, Springer-Verlag, pp. 356–365.

[3] R. S. Coulter and M. Henderson, *A class of functions and their application in constructing semi-biplanes and association schemes*, Discrete Math., 202 (1999), pp. 21–31.

[4] R. S. Coulter and R. W. Mathews, *Planar functions and planes of lenz-barlotti class II*, Des., Codes, Cryptogr., 10 (1997), pp. 167–184.

[5] P. Dembowski and T. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z., 103 (1968), pp. 239–258.

[6] H. Dobbertin, *One-to-one highly nonlinear power functions on $GF(2^n)$*, Appl. Algebra Eng. Commun. Comput., 9 (1998), pp. 139–152.

[7] ———, *Almost perfect nonlinear power functions on GF(2^n): The Niho case*, Information and Computation, 151 (1999), pp. 57–72.

[8] ———, *Almost perfect nonlinear power functions on GF(2^n): The Welch case*, IEEE Trans. Inf. Theory, 45 (1999), pp. 1271–1275.

[9] ———, *Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5*, in Proceedings of the conference on Finite Fields and Applications, Augsburg 1999, D. Jungnickel and H. Niederreiter, eds., New York, 2000, Springer-Verlag. to appear.

[10] T. Helleseth, C. Rong, and D. Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE Transactions on Information Theory, 45 (1999), pp. 475–485.

[11] T. Helleseth and D. Sandberg, *Some power mappings with low differential uniformity*, Applicable Algebra in Engineering, Communications and Computing, 8 (1997), pp. 363–370.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2nd ed., 1997.