Cryptography and Communications (2020) 12:841–857
https://doi.org/10.1007/s12095-020-00437-z

The multivariate method strikes again: New power functions with low differential uniformity in odd characteristic

Patrick Felke[1]

Received: 19 September 2019 / Accepted: 3 May 2020 / Published online: 16 May 2020

Abstract

Let $f(x) = x^d$ be a power mapping over $\mathbb{F}_n$ and $\mathcal{U}_d$ the maximum number of solutions $x \in \mathbb{F}_n$ of $\Delta_{f,c}(x) := f(x+c) - f(x) = a$, where $c, a \in \mathbb{F}_n$ and $c \neq 0$. f is said to be differentially k-uniform if $\mathcal{U}_d = k$. The investigation of power functions with low differential uniformity over finite fields $\mathbb{F}_n$ of odd characteristic has attracted a lot of research interest since Helleseth, Rong and Sandberg started to conduct extensive computer search to identify such functions. These numerical results are well-known as the Helleseth-Rong-Sandberg tables and are the basis of many infinite families of power mappings $x^{d_n}, n \in \mathbb{N}$, of low uniformity (see e.g. Dobbertin et al. Discret. Math. **267**, 95–112 2003; Helleseth et al. IEEE Trans. Inform Theory, **45**, 475–485 1999; Helleseth and Sandberg AAECC, **8**, 363–370 1997; Leducq Amer. J. Math. **1**(3) 115–123 1878; Zha and Wang Sci. China Math. **53**(8) 1931–1940 2010). Recently the crypto currency IOTA and Cybercrypt started to build computer chips around base-3 logic to employ their new ternary hash function Troika, which currently increases the cryptogrpahic interest in such families. Especially bijective power mappings are of interest, as they can also be employed in block- and stream ciphers. In this paper we contribute to this development and give a family of power mappings x^{d_n} with low uniformity over $\mathbb{F}_n$, which is bijective for $p \equiv 3 \bmod 4$. For $p = 3$ this yields a family x^{d_n} with $3 \leq \mathcal{U}_{d_n} \leq 4$, where the family of inverses has a very simple description. These results explain "open entries" in the Helleseth-Rong-Sandberg tables. We apply the multivariate method to compute the uniformity and thereby give a self-contained introduction to this method. Moreover we will prove for a related family of low uniformity introduced in Helleseth and Sandberg (**AAECC**, **8** 363–370 1997) that it yields permutations.

Keywords Almost perfect nonlinear · Differential cryptanalysis · Differential uniformity · Differential spectrum · Perfect nonlinear · Power function · Exponential sums · Quadratic Character

This article belongs to the Topical Collection: *Boolean Functions and Their Applications IV*
Guest Editors: Lilya Budaghyan and Tor Helleseth

✉ Patrick Felke
patrick.felke@hs-emden-leer.de

[1] University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden, Germany

Mathematics Subject Classification (2010) 06E30 · 11T23 · 94A60 · 11L99 · 94A99

1 Introduction

We assume that the reader is familiar with basic facts on finite fields. Lidl et al. [13] is a good reference. The finite field with p^n elements is denoted by $\mathbb{F}_n$. The cyclic group of invertible elements is denoted by $\mathbb{F}_n^\times$ and a generator ω of this group is called a primitive element. Throughout this paper p denotes an odd prime.

Definition 1.1 Let f be a mapping $f : \mathbb{F}_n \to \mathbb{F}_n$.

1. For $c \in \mathbb{F}_n$ the Δ-mapping of f with respect to c is defined as
$$\Delta_{f,c}(x) := f(x + c) - f(x).$$
2. $N_f(c, a)$ is defined as $\#\Delta_{f,c}^{-1}(a)$ for $a, c \in \mathbb{F}_n$, i.e. the number of solutions of $f(x + c) - f(x) - a = 0$.
3. The family $\left(N_f(c.a)\right)_{c,a\in\mathbb{F}_n}$ is called the difference spectrum.
4. We say that two mappings f and g have the same difference properties if the difference spectrum is equal up to a permutation, i.e. for all $a, c \in \mathbb{F}_n$ there exist $b, d \in \mathbb{F}_n$ with $N_f(c, a) = N_g(d, b)$ and vice versa.
5. The (differential) uniformity of f is $\mathcal{U}_f := \max\{N_f(c, a)|a, c \in \mathbb{F}_n, c \neq 0\}$.
6. A mapping f is called (differentially) k-uniform if $\mathcal{U}_f = k$.
7. If f is a power mapping x^d we will use the notation $\Delta_{d,c}(x)$, $N_d(c, a)$ and $\mathcal{U}_d$.

Remark 1.1 If $k = 1$, then f is called perfect nonlinear (PN) or planar. It is well-known that such functions exist only over finite field of odd characteristic. For an example see e.g. [4]. If $k = 2$, then f is called almost perfect nonlinear (APN). This is the best that can be achieved for even characteristic (see e.g. [7]).

When classifying mappings according to the above properties it is common to focus on the difference properties. The following equivalence relation from [2] is the most common and general known equivalence relation preserving the difference properties of two functions f and g.

Definition 1.2 Two mappings f, g from $\mathbb{F}_n$ to itself are called Carlet-Charpin-Zinoviev-equivalent (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_n^2$ the graph $\mathcal{L}(\Gamma_f)$ is equal to Γ_h, where the graph is defined as $\Gamma_M := \{(x, f(x))|x \in \mathbb{F}_n\}$ for a mapping M.

For power mappings we have the following simplification by Dempwolff [5].

Theorem 1.3 *Let $\mathbb{F}_n$ be a finite field of characteristic p and x^k and x^l be power functions on $\mathbb{F}_n$. Then x^k and x^l are CCZ-equivalent, if and only if there exists a positive integer $0 \leq m < n$, such that $l = p^m k \bmod (p^n - 1)$ or $kl = p^m \bmod (p^n - 1)$.*

Remark 1.2 It is well-known that a power mapping x^d is a permutation over $\mathbb{F}_n$ iff $\gcd(d, p^n - 1) = 1$. The inverse is given by $x^{d^{-1}}$, where d^{-1} is s.t. $d^{-1} \cdot d = 1 \bmod p^n - 1$. Note, that the latter condition in the above theorem means that $x^{p^{n-m}k}$ and x^l are inverse to each other. Moreover the theorem states that if x^d is a permutation with inverse $x^{d^{-1}}$ then these mappings have the same difference properties.

The following lemma is well-known (see e.g. [7])

Lemma 1.4 *For a power mapping x^d over $\mathbb{F}_n$ the difference spectrum is completely determined by considering $\Delta_{d,1}\left(x-\frac{1}{2}\right)=a, a\in\mathbb{F}_n$.*

Classifying mappings of low uniformity up to CCZ-equivalence is of interest in cryptography since differential and linear cryptanalysis exploit weaknesses of the uniformity of the functions which are used in AES and many other block ciphers. Helleseth, Rong and Sandberg conducted extensive computer search in the 90s to classify k-uniform power mappings. These numerical results are well-known as the Helleseth-Rong-Sandberg tables (H-R-S tables). Several inifinite families of mappings have been discovered since then and their uniformity determined in a series of papers thereby explaining some of these entries (see e.g. [7, 9, 10, 14, 15]).

For applications in cryptography, one would like to employ mappings f for which $\mathcal{U}_f$ is as small as possible. The proprietary hash function Curl employed in the cryptocurrency IOTA for example makes use of ternary S-Boxes and is vulnerable to differential cryptanalysis. After being broken the IOTA foundation developed in cooporation with Cybercrypt the ternary hash function Troika as its substitute and initiated a crypto challenge over 200.000 €. As the foundation is currently developing new computer chips built around base-3 logic, mappings with low uniformity over $\mathbb{F}_{3^n}$ have become cryptographically relevant (see [11]). In this context research on bijective power mappings with low uniformity over $\mathbb{F}_n$ and $\mathbb{F}_{3^n}$ in particular is of interest as they can be also employed in SPN- or stream ciphers. As mentioned before planar functions have the lowest possible uniformity of one and therefore cannot be bijective. Thus bijective mappings have necessarily a uniformity of at least two. That these can be still cryptograhically strong is well demonstrated for characteristic 2 by the block cipher AES.

1.1 Our contribution

In this paper we contribute to this development and give a family of power mappings x^{d_n} with low uniformity over $\mathbb{F}_n$, which is bijective for $p\equiv 3 \bmod 4$ and n odd. In case of $p=3$ we get a bijective family x^{d_n} of uniformity $\mathcal{U}_{d_n}\leq 4$, where the family $x^{d_n^{-1}}$ of inverses has a very simple description and is thus of particular interest for this new direction in cryptography. As a side result we will get that the mapping $x^{d_n}, d_n=\frac{p^n-1}{2}+2$ is bijective for $p\equiv 3 \bmod 4$ and n odd. Its uniformity was computed in [10].

1.2 Organization

This paper is organized as follows. In the next section we will introduce our results. Then we will give the mathematical background required for the proofs. In Section 4 we will introduce the multivariate method from [8] and compute the uniformity as well as the bijectivity in several subsections. In the final section we will discuss further research.

2 New power mappings of low uniformity

In this paper, we prove the following theorems.

Theorem 2.1 *Let $x^{d_n}, d_n=\frac{p^n-1}{2}+p^{\frac{n+1}{2}}+1$ be a power function from $\mathbb{F}_n$ to $\mathbb{F}_n$, $p\neq 3$ an odd prime and n odd. Then*

1. x^{d_n} *is a permutation for* $p \equiv 3 \bmod 4$.
2. $\mathcal{U}_{d_n} = 3$, *if* $p \equiv 1 \bmod 4$ *and either* $p \neq 17$ *or* $n > 1$,
3. $\mathcal{U}_{d_n} = 2$, *if* $p = 17$ *and* $n = 1$,
4. $\mathcal{U}_{d_n} \in \{4, 6\}$ *otherwise.*

Remark 2.1 Since $\frac{p^n-1}{2}$ is even for $p \equiv 1 \bmod 4$ the exponent d_n is even and thus $x^{d_n} = (-x)^{d_n}$. Therefore x^{d_n} cannot be a permutation in this case.

For $p = 3$ we have

Theorem 2.2 *The family* $x^{d_n}, d_n = \frac{3^n-1}{2} + 3^{\frac{n+1}{2}} + 1$ *is bijective with inverse* $x^{d'_n}$, *where*

$$d'_n = \begin{cases} \frac{3^{\frac{n+1}{2}}-1}{2}, n \equiv 1 \bmod 4 \\ \frac{3^n-1}{2} + \frac{3^{\frac{n+1}{2}}-1}{2}, n \equiv 3 \bmod 4 \end{cases}$$

and $\mathcal{U}_{d_n} = \mathcal{U}_{d'_n} \in \{3, 4\}$ *for* $n > 1$.
It is $\mathcal{U}_{d_n} = 3$ *for* $n = 1$.

The uniformity for $p = 5$ in theorem 2.1 and for the family in theorem 2.2 was already proven in [8], whereas the explicit and simple description of the family of inverses in theorem 2.2 is new. Note that swapping $n \equiv 1 \bmod 4$ and $n \equiv 3 \bmod 4$ in the definition of d'_n gives the mapping introduced in [7] proven to be APN in [14]. This mapping is no longer bijective. Statement 4 of theorem 2.1 cannot be narrowed in general and this theorem explains the following open entries in the H-R-S tables as Table 1 shows.

d in Table 1 is the cyclotomic cosetleader defined as

$$\min\left(\{d \cdot p^i \bmod (p^n - 1) | 0 \leq i \leq n-1\}\right).$$

As this family explains open entries in the H-R-S table it is not CCZ-equivalent to known ones. It can also be seen as a generalization for odd n of the family $x^{d_n}, d_n = \frac{p^n-1}{2} + 2$ treated in [10]. Therefore it is not surprising that we will also prove the following theorem

Theorem 2.3 *The family of power mappings* $x^{d_n}, d_n = \frac{p^n-1}{2} + 2$ *is bijective for* $p \equiv 3 \bmod 4$ *and* n *odd.*

It was shown in [10] that its uniformity is 4.

Table 1 Open cases

p	n	d	uniformity	H-R-S entry
7	1	5	4	no H-R-S table
7	3	179	4	open H-R-S entry
7	5	8453	6	no H-R-S table
7	7	412115	6	no H-R-S table
11	1	7	2	no H-R-S table
11	3	677	4	open H-R-S entry
11	5	80647	6	no H-R-S table

In [8] it was shown that the family from theorem 2.2 is not CCZ-equivalent to known ones.

3 Preliminaries

The univariate polynomial ring over a finite field is denoted by $\mathbb{F}_n[x]$. The polynomial ring in two variables x, y over $\mathbb{F}_n$ is denoted by $\mathbb{F}_n[x, y]$. We will need the following facts about quadratic characters. A detailed treatment on the theory of characters can be found in [12] or [13].

The quadratic character over $\mathbb{F}_n$ is the mapping $\chi_{p^n} : \mathbb{F}_n \to \{-1, 0, 1\} \subset \mathbb{C}$ which can be by common abuse of language represented by the power mapping $\chi_{p^n}(x) = x^{\frac{p^n-1}{2}}$. This mapping has the following properties

$$\chi_{p^n}(\alpha) = \begin{cases} 0, & \text{if } \alpha = 0, \\ 1, & \text{iff } x^2 - \alpha = 0 \text{ has a solution in } \mathbb{F}_n^\times, \\ -1 & \text{otherwise.} \end{cases}$$

The following two propositions play a central role in this paper.

Proposition 3.1 1. *We have $\chi_{p^n}(-1) = 1$ iff $\frac{p^n-1}{2}$ is even.*
2. *If n is odd then $\chi_{p^n}(-1) = 1$ iff $p \equiv 1$ mod 4.*
3. *$\chi_{p^n}(a \cdot b) = \chi_{p^n}(a)\chi_{p^n}(b)$ for all $a, b \in \mathbb{F}_n$.*

If p is clear from the context we will just write χ_n.

Proposition 3.2 *If the equation $x^{p-1} = a, a \in \mathbb{F}_n^\times$ has a $p-1$-th root α over $\mathbb{F}_n$ then it has exactly $p-1$ roots. These are given by $\omega^i\alpha, i = 0, \ldots, p-2$, ω a primitive element of $\mathbb{F}_{p^\times}$.*

Proof As $a \neq 0$ the same is true for the solution α. Obviously $\omega^i\alpha, i = 0, \ldots, p-2$ are $p-1$ pairwise different solutions of $x^{p-1} = a$ or $x^{p-1} - a = 0$ respectively. As a polynomial of degree $p-1$ has at most $p-1$ zeros the assertion follows. □

The Weil estimate (see [13], p. 225, [1], p. 183) on character sums given in the next theorem is particularly useful to prove that certain character sums are non-zero, which are often encountered when computing the uniformity of power mappings.

Theorem 3.3 *Let $f(x) \in \mathbb{F}_n[x]$ be a polynomial with m distinct zeros in its splitting field, which is not a square of another polynomial, then*

$$\left| \sum_{\alpha \in \mathbb{F}_n} \chi_n(f(\alpha)) \right| \leq (m-1)\sqrt{p^n}.$$

If $f(x)$ has degree 2 it is

$$\left| \sum_{\alpha \in \mathbb{F}_n} \chi_n(f(\alpha)) \right| \leq 1.$$

With Tr_n we denote the trace function from $\mathbb{F}_n$ onto $\mathbb{F}_p$, which is given by

$$Tr_n(x) = x^{p^{n-1}} + \cdots + x^p + x.$$

The trace is linear and its kernel, which will be of interest here, has been parametrized by Hilbert in its famous theorem Hilbert 90 which is given below.

Theorem 3.4 *It is* $Tr_n(\gamma) = 0$ *iff* $\gamma = \alpha^p - \alpha, \alpha \in \mathbb{F}_n$.

Remark 3.1 Note that the mapping $x^p - x$ is $p-$to-1 over $\mathbb{F}_n$, because it is linear with kernel $\mathbb{F}_p$.

The proof based on the multivariate method requires to determine the zeros of multivariate equations in two unknowns which explains its name. Systematic methods for solving such equations are given in e.g. classical elimination theory. An important algebraic tool in this theory is the well-known resultant of $f(x, y)$ and $g(x, y)$, $f, g \in \mathbb{F}_n[x, y]$ with respect to y, which we denote by $\text{res}(f, g, y)$. We will make use of the next proposition which states how the resultant can be used for determining the solutions of a system of polynomial equations.

Proposition 3.5 *Given* $f(x, y), g(x, y) \in \mathbb{F}_n[x, y] \setminus \{0\}$.

1. $res(f, g, y) \in \mathbb{F}_n[x]$.
2. *There are polynomials* $p, q \in \mathbb{F}_n[x, y]$ *such that*

$$pf + qg = res(f, g, y)$$

and therefore the system of equations

$$\begin{aligned} f(x, y) &= 0 \\ g(x, y) &= 0 \end{aligned}$$

has a solution (α, β) *over a proper field extension only if* $res(f, g, y)(\alpha) = 0$.

For further reading on the resultant and elimination theory we refer to [3].

4 The multivariate method: Proof of Theorem 2.1

In this section we prove theorem 2.1 and thereby giving a simple and self-contained introduction to the multivariate method.

4.1 The multivariate representation

Recall that by theorem 1.3 and lemma 1.4 we can restrict to consider

$$\Delta_{d_n,1}\left(x - \frac{1}{2}\right) = a.$$

The first step is to express this equation as a system of multivariate equations.

To this end we denote the conjugation (Galois automorphism) $x \mapsto x^{p^{\frac{n+1}{2}}}$ by x^* and set $y := x^*$. Then it is

$$y^* = x^p$$

over $\mathbb{F}_n$ and

$$y = x$$

over $\mathbb{F}_p$. The latter property will be very useful later. Analogously we set $a^* = b$.

We get

$$x^{d_n} = \chi_n(x)yx$$

and the Δ-mapping can be represented by

$$F_1 : \chi_n\left(x+\frac{1}{2}\right)\left(y+\frac{1}{2}\right)\left(x+\frac{1}{2}\right) - \chi_n\left(x-\frac{1}{2}\right)\left(y-\frac{1}{2}\right)\left(x-\frac{1}{2}\right) = a. \quad (1)$$

By conjugation of F_1 with * we get

$$F_2 : \chi_n\left(x+\frac{1}{2}\right)\left(y+\frac{1}{2}\right)\left(x^p+\frac{1}{2}\right) - \chi_n\left(x-\frac{1}{2}\right)\left(y-\frac{1}{2}\right)\left(x^p-\frac{1}{2}\right) = b \quad (2)$$

as $\chi_n\left(x \pm \frac{1}{2}\right)^* = \chi_n\left(x \pm \frac{1}{2}\right)$.

We make a case distinction according to the 4 possible values of $\chi_n(x+\frac{1}{2})$, $\chi_n(x-\frac{1}{2})$ to get the sought for representation.

Case 1: $\chi_n\left(x-\frac{1}{2}\right) = 1, \chi_n\left(x+\frac{1}{2}\right) = 1$

$$F_{11} : x + y - a = 0 \quad (3)$$
$$F_{12} : x^p + y - b = 0$$

Case 2: $\chi_n\left(x-\frac{1}{2}\right) = -1, \chi_n\left(x+\frac{1}{2}\right) = 1$

$$F_{21} : xy - \frac{1}{2}a + \frac{1}{4} = 0 \quad (4)$$
$$F_{22} : x^p y - \frac{1}{2}b + \frac{1}{4} = 0$$

Case 3: $\chi_n\left(x-\frac{1}{2}\right) = 1, \chi_n\left(x+\frac{1}{2}\right) = -1$

$$F_{31} : xy + \frac{1}{2}a + \frac{1}{4} = 0 \quad (5)$$
$$F_{32} : x^p y + \frac{1}{2}b + \frac{1}{4} = 0$$

Case 4: $\chi_n\left(x-\frac{1}{2}\right) = -1, \chi_n\left(x+\frac{1}{2}\right) = -1$

$$F_{41} : x + y + a = 0 \quad (6)$$
$$F_{42} : x^p + y + b = 0$$

The above case distinction does not capture the cases $x = \pm\frac{1}{2}$ as $\chi_n\left(\frac{1}{2}-\frac{1}{2}\right) = \chi_n\left(-\frac{1}{2}+\frac{1}{2}\right) = 0$. We have

$$\chi_n\left(\frac{1}{2}+\frac{1}{2}\right)\left(\frac{1}{2}+\frac{1}{2}\right)\left(\frac{1}{2}+\frac{1}{2}\right) - \chi_n\left(\frac{1}{2}-\frac{1}{2}\right)\left(\frac{1}{2}-\frac{1}{2}\right)\left(\frac{1}{2}-\frac{1}{2}\right) = \chi_n(1)\cdot 1 = 1 \quad (7)$$

and

$$\chi_n\left(-\frac{1}{2}+\frac{1}{2}\right)\left(-\frac{1}{2}+\frac{1}{2}\right)\left(-\frac{1}{2}+\frac{1}{2}\right)- \tag{8}$$
$$\chi_n\left(-\frac{1}{2}-\frac{1}{2}\right)\left(-\frac{1}{2}-\frac{1}{2}\right)\left(-\frac{1}{2}-\frac{1}{2}\right)=-\chi_n(-1)=\pm 1.$$

by proposition 3.1. This gives the exceptional cases $a = \pm 1$. We will see that $a = \pm\frac{1}{2}$ will lead to exceptional cases as well. These lie all in the base field $\mathbb{F}_p$. From now on we assume $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ and treat $a \in \mathbb{F}_p$ in Section 4.4.

The principle of the multivariate method is now to compute the solutions of $F_{i1}, F_{i2}, i = 1, \ldots, 4$ with elementary elimination theory. Thereby we are only interested in solutions of the form (α, α^*). We call $F_{i1}, F_{i2}, i = 1, \ldots, 4$ fundamental equations and the above solutions suitable in the sequel as exactly these yield solutions of $\Delta_{d_n,1}(x - \frac{1}{2}) = a$ when the corresponding character condition is fulfilled. In this case the solution is called an actual solution. It will turn out that identifying suitable solutions for this type of power mappings can be done by uniform techniques and usually gives a tight upper bound on the uniformity. This makes the multivariate method to a powerful universal tool to study the uniformity. The problem of determining if the corresponding character condition is fulfilled for a suitable solution, i.e. if it is an actual solution, is much harder in general. The corresponding underlying mathematical problem to do so is easier described by the notion of a suitable solution as we will see. This explains why we distinguish between these types of solutions (see also Section 5).

One possibility to determine suitable solutions is to compute the resultant $\mathrm{res}(F_{i,1}, F_{i,2}, y)$ (by abuse of language) of the left hand side of the fundamental equations with respect to y. This can be seen as follows.

By proposition 3.5 the equation $\Delta_{d_n,1}(x - \frac{1}{2}) = a$ has a suitable solution α only if α is a zero of one of the above $\mathrm{res}(F_{i,1}, F_{i,2}, y)$. Then one shows which of the zeros α yield suitable solutions. Moreover as long as we do not encounter an exceptional case for the quadratic character any solution belongs exactly to one of the four cases. Therefore the above resultants are called fundamental polynomials. In general the resultant can be computed very easily with the help of computer algebra systems like `magma`.

Note that all suitable solutions (α, α^*) of F_{i1}, F_{i2}, when considered as a system of multivariate equations yield a zero α of the resultant but not the other way around. There might exist zeros α of the resultant which do not extend to solutions of F_{i1}, F_{i2} at all. All other zeros α extend to a solution (α, β) of F_{i1}, F_{i2} but β is not necessarily equal to α^*. Therefore not all zeros of $\mathrm{res}(F_{i,1}, F_{i,2}, y)$ yield suitable solutions and not all suitable solutions result in actual solutions. In principle any univariate polynomial $\phi_i(x)$ with $\phi_i(\alpha) = 0$ for all actual solutions (α, α^*) of F_{i1} can be employed in the multivariate method. Therefore we call $\phi_i(x)$ a fundamental polynomial in the sequel. Here we compute such a $\phi_i(x)$ by hand e.g.

$$\phi_1(x) = F_{12} - F_{11} \text{ and } \phi_2(x) = \left(\frac{1}{\left(-\frac{1}{2}a+\frac{1}{4}\right)}\left(x^{p-1}\cdot F_{21} - F_{22}\right)\right).$$

The latter computation is defined as long as $a \neq \frac{1}{2}$, which we excluded. The exceptional case $a = -\frac{1}{2}$ comes into play by computing ϕ_3 in the same vein. We get

Case 1: $\chi_n\left(x-\frac{1}{2}\right)=1, \chi_n\left(x+\frac{1}{2}\right)=1$

$$\phi_1(x) := x^p - x + a - b \tag{9}$$

Case 2: $\chi_n\left(x-\frac{1}{2}\right)=-1, \chi_n\left(x+\frac{1}{2}\right)=1$

$$\phi_2(x) := \left(x^{p-1} - \frac{b-\frac{1}{2}}{a-\frac{1}{2}}\right), a \neq \frac{1}{2} \tag{10}$$

Case 3: $\chi_n\left(x-\frac{1}{2}\right)=1, \chi_n\left(x+\frac{1}{2}\right)=-1$

$$\phi_3(x) := \left(x^{p-1} - \frac{b+\frac{1}{2}}{a+\frac{1}{2}}\right), a \neq -\frac{1}{2} \tag{11}$$

Case 4: $\chi_n\left(x-\frac{1}{2}\right)=-1, \chi_n\left(x+\frac{1}{2}\right)=-1$

$$\phi_4(x) := x^p - x - a + b \tag{12}$$

4.2 The contribution of ϕ_1 and ϕ_4, $a \in \mathbb{F}_n \setminus \mathbb{F}_p$

By 3.4 and remark 3.1 the fundamental polynomials $\phi_1(x), \phi_4(x)$ split over $\mathbb{F}_n$ as $Tr_n(\pm(b-a))=0$ and the zeros of ϕ_1 and ϕ_4 can be represented as

$$\alpha+\beta \text{ and } -(\alpha+\beta) \text{ respectively,}$$

where $\phi_1(\alpha)=0$ and $\beta \in \mathbb{F}_p$. We will show that ϕ_1 contributes exactly one suitable solution. To do so we prove at first that ϕ_1 contributes at most one suitable solution. Assume the contrary. Then there exist $\beta_1, \beta_2 \in \mathbb{F}_p$ with

$$\alpha+\beta_1+\alpha^*+\beta_1^*=a$$

and

$$\alpha+\beta_2+\alpha^*+\beta_2^*=a.$$

Subtracting both equations gives

$$\beta_1-\beta_2+(\beta_1-\beta_2)^*=0.$$

As $\beta_1-\beta_2 \in \mathbb{F}_p$ it is $(\beta_1-\beta_2)^*=(\beta_1-\beta_2)$. Consequently

$$\beta_1-\beta_2+(\beta_1-\beta_2)^*=2\cdot(\beta_1-\beta_2)=0.$$

It follows $\beta_1-\beta_2=0$ and thus $\beta_1=\beta_2$, which contradicts our assumption.

Now consider the linear mapping $L: x \mapsto x+x^*$ over $\mathbb{F}_n$. Any element α in the preimage of $L^{-1}(a), a \in \mathbb{F}_{p^n} \setminus \mathbb{F}_p$ yields a suitable solution of $x+y=x+x^*=a$ and vice versa. It follows that $\#L^{-1}(a) \leq 1$. Moreover the mapping is equal to $2x$ over $\mathbb{F}_p$ as in this case $x^*=x$.. Thus the mapping is injective over the whole field $\mathbb{F}_n$ and therefore L is a permutation. From this it follows that ϕ_1 contributes exactly one suitable solution (over the whole field $\mathbb{F}_n$).

A direct consequence is that the fundamental (6) has exactly one suitable solution as well, which is equal to $-(\alpha+\beta)$ where $\alpha+\beta$ denotes the suitable solution of (3). We have

$$\chi_n\left(-x-\frac{1}{2}\right)=\chi_n(-1)\chi_n\left(x+\frac{1}{2}\right) \text{ and } \chi_n\left(-x+\frac{1}{2}\right)=\chi_n(-1)\chi_n\left(x-\frac{1}{2}\right).$$

From this it follows together with proposition 3.1 and the fact that the suitable solutions of (3) and (6) differ by a sign:

1. If $p \equiv 3 \bmod 4$ then for all $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ there exists exactly one $\alpha + \beta_0, \beta_0 \in \mathbb{F}_p$ of $\phi_1(x)$, which yields a suitable solution of the fundamental (3) and the corresponding $-(\alpha + \beta_0)$ extends to the only suitable solution of the fundamental (6).

   Moreover it is $\chi_n(-1) = -1$ and therefore $\alpha + \beta_0, -(\alpha + \beta_0)$ yield 2 actual solutions iff $\chi_n(\alpha + \beta_0 - \frac{1}{2}) = \chi_n(\alpha + \beta_0 + \frac{1}{2}) = 1$ and 0 otherwise.
2. If $p \equiv 1 \bmod 4$ then for all $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ there exists exactly one zero $\alpha + \beta_0$ of $\phi_1(x)$, which yields a suitable solution of the fundamental (3) and the corresponding $-(\alpha + \beta_0)$ extends to the only suitable solution of the fundamental (6).

   Here $\chi_n(-1) = 1$ and therefore either $\alpha + \beta_0$ or $-(\alpha + \beta_0)$ yields to 1 actual solution iff either $\chi_n(\alpha + \beta_0 - \frac{1}{2}) = \chi_n(\alpha + \beta_0 + \frac{1}{2}) = 1$ or $\chi_n(\alpha + \beta_0 - \frac{1}{2}) = \chi_n(\alpha + \beta_0 + \frac{1}{2}) = -1$ and 0 otherwise.

4.3 The contribution of ϕ_2 and ϕ_3, $a \in \mathbb{F}_n \setminus \mathbb{F}_p$

We have that $p^{\frac{n+1}{2}} - 1$ is always divisible by $p - 1$ which follows directly from the general identity $p^l - 1 = (p-1)\sum_{i=0}^{l-1} p^i, l \in \mathbb{N}$. Therefore for $a \in \mathbb{F}_n$

$$\left(a - \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}$$

is a $(p-1)$-th root of $\frac{b-\frac{1}{2}}{a-\frac{1}{2}}$. By proposition 3.2 ϕ_2 splits over $\mathbb{F}_n$ as follows

$$\phi_2(x) = \left(x - \omega^0\left(a - \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right) \cdot \cdots \cdot \left(x - \omega^{p-2}\left(a - \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right), \omega \in \mathbb{F}_p^{\times}. \quad (13)$$

Analogously we have

$$\phi_3(x) = \left(x - \omega^0\left(a + \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right) \cdot \cdots \cdot \left(x - \omega^{p-2}\left(a + \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right), \omega \in \mathbb{F}_p^{\times}. \quad (14)$$

Plugging $\omega^i \left(a - \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}$ into the left hand side of the fundamental (4) and making use of $xy = x^2$ over $\mathbb{F}_p$ gives

$$\omega^{2i}\left(a - \frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}\cdot\left(p^{\frac{n+1}{2}}+1\right)} = \omega^{2i}\left(a - \frac{1}{2}\right)^{\frac{(p-1)\cdot p^n + p^n - 1}{p-1}}$$

$$= \omega^{2i}\left(a - \frac{1}{2}\right)\left(a - \frac{1}{2}\right)^{\frac{p^n-1}{p-1}} = \omega^{2i}\left(a - \frac{1}{2}\right)^{\frac{p^n-1}{p-1}}\left(a - \frac{1}{2}\right). \quad (15)$$

Thus fundamental (4) is fulfilled iff $\omega^{2i}\left(a - \frac{1}{2}\right)^{\frac{p^n-1}{p-1}} = \frac{1}{2}$ i.e.

$$\omega^{2i} = \frac{1}{2}\left(a - \frac{1}{2}\right)^{-\frac{p^n-1}{p-1}}, \quad (16)$$

for a proper chosen $0 \leq i \leq p-2$ as by assumption $\left(a-\frac{1}{2}\right) \neq 0$. We have $\left(\left(a-\frac{1}{2}\right)^{-\frac{p^n-1}{p-1}}\right)^{p-1} = 1$ and conclude that the right hand side of (16) lies in $\mathbb{F}_p$. Since the quadratic character is a homomorphism with respect to multiplication (see proposition 3.1) and $\frac{p^n-1}{p-1} = \sum_{j=0}^{n-1} p^j$ is odd we get $\chi_n\left(\left(a-\frac{1}{2}\right)^{\frac{p^n-1}{p-1}}\right) = \chi_n(a-\frac{1}{2})$. Therefore such an i exists iff $\chi_n\left(\frac{1}{2}\left(a-\frac{1}{2}\right)\right) = 1$ as ω^{2i} runs through all squares in $\mathbb{F}_p$ for $0 \leq i \leq p-2$. Moreover since x^2 is 2-to-1 over $\mathbb{F}_p$ (16) has exactly two solutions. These are denoted by $\pm\omega^{i_n}$. It follows that the possible suitable solutions of the fundamental (4) are

$$\pm\,\omega^{i_n}\left(a-\frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}} \tag{17}$$

Analogously one shows that the fundamental (5) has two suitable solutions iff $\chi_n\left(-\frac{1}{2}\left(a+\frac{1}{2}\right)\right) = 1$. In this case the two suitable solutions of the fundamental (5) are

$$\pm\,\omega^{i_n}\left(a+\frac{1}{2}\right)^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}, \tag{18}$$

where $i_n \in \{0, \ldots, p-2\}$ is s.t.

$$\omega^{2i_n} = \left(-\frac{1}{2}\right)\left(a+\frac{1}{2}\right)^{-\frac{p^n-1}{p-1}}.$$

Recall that $\chi_n\left(-x-\frac{1}{2}\right) = \chi_n(-1)\chi_n\left(x+\frac{1}{2}\right)$ and $\chi_n\left(-x+\frac{1}{2}\right) = \chi_n(-1)\chi_n\left(x-\frac{1}{2}\right)$. Thus we get in dependence of $p \bmod 4$:

1. If $p \equiv 3 \bmod 4$ then the fundamental (4) has exactly two suitable solutions iff $\chi_n\left(\frac{1}{2}\left(a-\frac{1}{2}\right)\right) = 1$.

   We have $\chi_n(-1) = -1$ and therefore the suitable solutions yield actual solutions iff additionally the character condition is fulfilled for one and thus both solutions given in (17) and 0 actual solutions otherwise.

   Analogously one gets that the fundamental (5) has 2 actual solutions iff $\chi_n\left(-\frac{1}{2}\left(a+\frac{1}{2}\right)\right) = 1$ and the character condition is fulfilled for one and thus both of the 2 solutions given in (18) and 0 otherwise.
2. If $p \equiv 1 \bmod 4$ then the fundamental (4) has two suitable solutions iff $\chi_n\left(\frac{1}{2}\left(a-\frac{1}{2}\right)\right) = 1$ as in the other case.

   We have $\chi_n(-1) = 1$ and therefore at most one of the two suitable solutions given in (17) fulfills the character condition.

   Thus (4) has exactly 1 actual solution iff $\chi_n\left(\frac{1}{2}\left(a-\frac{1}{2}\right)\right) = 1$ and the character condition is fulfilled for one of the two suitable solutions given in (17) and 0 solutions otherwise.

   Analogously one gets that (5) has exactly 1 actual solution iff $\chi_n\left(-\frac{1}{2}\left(a+\frac{1}{2}\right)\right) = 1$ and the character condition is fulfilled for one of the two possible zeros given in (18) and 0 solutions otherwise.

4.4 Exceptions $a \in \mathbb{F}_p$

Over the base field $\mathbb{F}_p$ it is $b = a$. Applying the multivariate method by taking this into account yields

Case 1: $\chi(x - \frac{1}{2}) = 1, \chi(x + \frac{1}{2}) = 1$

$$F_{11} : x + y - a = 0 \tag{19}$$
$$F_{12} : x^p + y - a = 0 \tag{20}$$

Case 2: $\chi(x - \frac{1}{2}) = -1, \chi(x + \frac{1}{2}) = 1$

$$F_{21} : xy - \frac{1}{2}a + \frac{1}{4} = 0 \tag{21}$$
$$F_{22} : x^p y - \frac{1}{2}a + \frac{1}{4} = 0$$

Case 3: $\chi(x - \frac{1}{2}) = 1, \chi(x + \frac{1}{2}) = -1$

$$F_{31} : xy + \frac{1}{2}a + \frac{1}{4} = 0 \tag{22}$$
$$F_{32} : x^p y + \frac{1}{2}a + \frac{1}{4} = 0$$

Case 4: $\chi\left(x - \frac{1}{2}\right) = -1, \chi\left(x + \frac{1}{2}\right) = -1$

$$F_{41} : x + y + a = 0 \tag{23}$$
$$F_{42} : x^p + y + a = 0$$

We get

$$\phi_1(x) = \phi_4(x) = x^p - x,$$
$$\phi_2(x) = x^{p-1}F_{21} - F_{22} = -\frac{1}{2}a + \frac{1}{4}\left(x^{p-1} - 1\right)$$

and

$$\phi_3(x) = x^{p-1}F_{31} - F_{32} = \frac{1}{2}a + \frac{1}{4}\left(x^{p-1} - 1\right).$$

Obviously all zeros of $\phi_1, \ldots, \phi_4$ lie in $\mathbb{F}_p$. Note that for $a = \pm 1$ we enter the exceptional cases for the character conditions treated in (7) and (8). We conclude that if $a \in \mathbb{F}_p$ then the preimage

$$\Delta_{1,d_n}\left(x - \frac{1}{2}\right)^{-1}(a) \subset \mathbb{F}_p.$$

Thus we can restrict to consider x^{d_n} over $\mathbb{F}_p$. As $x^{d_n} = \chi_1(x)x^2$ over $\mathbb{F}_p$ we can apply theorem 3 and the remark on p. 368 of [10], which together state that

$$\mathcal{U}_{d_n} = \begin{cases} 4, \text{ if } p \equiv 3 \bmod 4 \text{ and } p \neq 3, \\ 3, \text{ if } p \equiv 1 \bmod 4 \text{ and either } p \neq 17 \text{ or } n > 1, \\ 2, \text{ if } p = 17. \end{cases}$$

over the base fields.

4.5 Combining all results

From what we have proven so far we get:

If $p \equiv 3 \bmod 4$ then

1. if $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ then $\Delta_{1,d_n}(x - \frac{1}{2}) = a$ has either 0 or 2 actual solutions coming from the fundamental (3) and (6).
2. if $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ it has 0, 2 or 4 actual solutions from the fundamental (4) and (5).
3. if $a \in \mathbb{F}_p$, $p \neq 3$ then $\Delta_{1,d_n}(x - \frac{1}{2}) = a$ has at most 4 actual solutions and the value 4 is assumed.

It follows that $\mathcal{U}_{d_n} \in \{4, 6\}$ for $p \neq 3$.

If $p \equiv 1 \bmod 4$ then

1. if $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ then $\Delta_{1,d_n}(x - \frac{1}{2}) = a$ has 0 or 1 actual solution from the fundamental (3) and (6).
2. if $a \in \mathbb{F}_n \setminus \mathbb{F}_p$ it has 0, 1 or 2 actual solutions from (4) and (5).
3. if $a \in \mathbb{F}_p$ then $\Delta_{1,d_n}(x - \frac{1}{2}) = a$ has at most 3 actual solutions if either $p \neq 17$ or $n > 1$ and the value 3 is assumed in these cases.
4. if $a \in \mathbb{F}_p$, $p = 17$ then $\Delta_{1,d_n}(x - \frac{1}{2}) = a$ has at most 2 actual solutions and the value 2 is assumed.

It follows that $\mathcal{U}_{d_n} = 2$ if $p = 17$ and $n = 1$ and $\mathcal{U}_{d_n} = 3$ otherwise. This ends the proof of the uniformity part of theorem 2.1.

4.6 Proof of the permutation property for $p \equiv 3 \bmod 4$ and Theorem 2.3

By remark 1.2 the mapping x^{d_n}, $d_n = \frac{p^n-1}{2} + p^{\frac{n+1}{2}} + 1$ is a permutation iff $\gcd(d_n, p^n - 1) = 1$, which is what we will show now.

As $\frac{p^n-1}{2}$ is odd also d_n odd. Thus any element dividing d_n and $p^n - 1$ is odd and therefore divides $\frac{p^n-1}{2}$. Hence it also divides $d_n - \frac{p^n-1}{2} = p^{\frac{n+1}{2}} + 1$. It follows that

$$\gcd(d_n, p^n - 1) = \gcd\left(p^{\frac{n+1}{2}} + 1, \frac{p^n - 1}{2}\right) = \frac{\gcd\left(p^{\frac{n+1}{2}} + 1, p^n - 1\right)}{2}. \tag{24}$$

We will show that $\gcd\left(p^{\frac{n+1}{2}} + 1, p^n - 1\right)$ equals 2. From this the assertion follows.

Multiplying $p^{\frac{n+1}{2}} + 1$ by $p^{\frac{n-1}{2}} - 1$ and subtracting $p(p^n - 1)$ gives $-p + 1$. Therefore the above gcd divides $p - 1$. It is

$$p^{\frac{n+1}{2}} + 1 = p^{\frac{n+1}{2}} - 1 + 2 = (p - 1)\sum_{i=0}^{\frac{n-1}{2}} p^i + 2.$$

As the gcd divides $p - 1$ it also divides $(p - 1)\sum_{i=0}^{\frac{n-1}{2}} p^i$ and consequently the difference

$$(p - 1)\sum_{i=0}^{\frac{n-1}{2}} p^i + 2 - (p - 1)\sum_{i=0}^{\frac{n-1}{2}} p^i = 2.$$

Thus $\gcd(p^{\frac{n+1}{2}} + 1, p^n - 1) = 2$ and from the identity given in (24) the permutation property follows.

In the same vein Theorem 2.3 is proved.

This ends the proof of the Theorem 2.1 and Theorem 2.3.

4.7 Proof of Theorem 2.2

4.7.1 Proof of the permutation property

At first we will show that $x^{d'_n}$, where

$$d'_n = \begin{cases} \frac{3^{\frac{n+1}{2}}-1}{2}, n \equiv 1 \bmod 4 \\ \frac{3^n-1}{2} + \frac{3^{\frac{n+1}{2}}-1}{2}, n \equiv 3 \bmod 4 \end{cases}$$

is the inverse of x^{d_n}. We will prove the case $n \equiv 3 \bmod 4$ by showing that $d_n \cdot d'_n = 1 \bmod 3^n - 1$. From this the assertion follows for this case. We have

$$\frac{3^{\frac{n+1}{2}}-1}{2} = \sum_{i=0}^{\frac{n-1}{2}} 3^i,$$

which is even as $\frac{n-1}{2}$ is odd for $n \equiv 3 \bmod 4$. Therefore d'_n is odd.

We have

$$d_n \cdot d'_n = \left(\tfrac{3^n-1}{2}\right)\left(\tfrac{3^n-1}{2} + \tfrac{3^{\frac{n+1}{2}}-1}{2}\right) + \left(3^{\frac{n+1}{2}}+1\right)\left(\tfrac{3^n-1}{2} + \tfrac{3^{\frac{n+1}{2}}-1}{2}\right) \bmod 3^n - 1.$$

As d'_n is odd it is $x^{\frac{3^n-1}{2}d'_n} = \chi_n(x)^{d'_n} = \chi_n(x)$. We get that

$$\frac{3^n-1}{2} d'_n = \frac{3^n-1}{2} \bmod 3^n - 1.$$

The second term of the sum is equal to

$$\left(3^{\frac{n+1}{2}}+1\right)\left(\frac{3^n-1}{2}\right) + 1 + \frac{3^n-1}{2} \bmod 3^n - 1. \tag{25}$$

We have that $3^{\frac{n+1}{2}} + 1$ is even and therefore

$$x^{\left(3^{\frac{n+1}{2}}+1\right)\left(\frac{3^n-1}{2}\right)} = \chi_n(x)^{3^{\frac{n+1}{2}}+1} = 1 = x^0$$

over $\mathbb{F}_n^\times$. Thus (25) simplifies to $1 + \frac{3^n-1}{2} \bmod 3^n - 1$. The addition of both simplifications gives

$$d_n \cdot d'_n = 1 + \frac{3^n-1}{2} + \frac{3^n-1}{2} = 1 \bmod 3^n - 1$$

as requested.

The case $n \equiv 1 \bmod 4$ is proven analogously.

4.7.2 Proof of $3 \leq \mathcal{U}_{d_n} \leq 4$

A direct computation shows that the $\mathcal{U}_{d_1} = 3$.

The proof for $n > 1$ is exactly as in the general case. Therefore we restrict to prove that ϕ_2 and ϕ_3 never contribute a suitable solution at the same time. Then from what we have proven in Sections 4.3 and 4.4 adapted to $p = 3$ it follows that $3 \leq \mathcal{U}_{d_n} \leq 4$.

In the case $p = 3$ the zeros of ϕ_2 and ϕ_3 are the roots

$$\pm (a+1)^{\frac{3^{\frac{n+1}{2}}-1}{2}}$$

and

$$\pm (a-1)^{\frac{3^{\frac{n+1}{2}}-1}{2}}.$$

From Section 4.3 we get that the two roots of $\phi_2(x)$ yield suitable solutions of fundamental (4) only if $\chi(-a-1) = 1$ which simplifies to $\chi(a+1) = -1$ since $\chi(-1) = -1$. Moreover the suitable solutions fulfill the character condition $\chi(x+1) = -1$, $\chi(x-1) = 1$ only if

$$\chi_n\left(\left(\pm (a+1)^{\frac{3^{\frac{n+1}{2}}-1}{2}} + 1\right) \cdot \left(\pm (a+1)^{\frac{3^{\frac{n+1}{2}}-1}{2}} - 1\right)\right) =$$

$$\chi_n\left(\frac{b+1}{a+1} - 1\right) = \chi_n\left(\frac{b-a}{a+1}\right) = -1.$$

Therefore ϕ_2 contributes two actual solutions only if $\chi_n(b-a) = 1$. Similarly one shows, that ϕ_3 contributes two actual solutions only if $\chi_n(a-1) = 1$ and $\chi_n\left(\frac{b-a}{a-1}\right) = -1$, which leads to $\chi_n(b-a) = -1$. We conclude that ϕ_2 and ϕ_3 never contribute actual solutions at the same time as long as $a \neq \pm 1$. This case is covered by the above direct computation as again we have that $\Delta_{d_n,1}(x - \frac{1}{2})^{-1}(a) \subset \mathbb{F}_3$ for $a \in \mathbb{F}_3$. As the mapping has uniformity 3 over $\mathbb{F}_3$ it follows that $\mathcal{U}_{d_n} \in \{3, 4\}$. This proves the corollary.

A question arising is if we are able to compute the exact uniformity for $n > 1$. In [8] it was shown that from what we have proven so far we get that $\mathcal{U}_{d_n} = 4$ for $\mathbb{F}_{3^n}$, $n > 1$ iff the following character sum is non-zero.

$$\frac{1}{2^5}\sum_{\alpha\in\mathbb{F}_n}(1+\chi_n(\alpha+1))(1+\chi_n(\alpha-1))(1-\chi_n(\alpha))\cdot \left(1+\chi_n\left(\left(\alpha+\alpha^{3^{\frac{n+1}{2}}}+1\right)^{\frac{3^{\frac{n+1}{2}}-1}{2}}-1\right)\right)\cdot \left(1-\chi_n\left(\left(\alpha+\alpha^{3^{\frac{n+1}{2}}}+1\right)^{\frac{3^{\frac{n+1}{2}}-1}{2}}+1\right)\right) \tag{26}$$

Standard techniques to prove that such a character sum is non-zero make use of the Weil bound (see theorem 3.3). This bound is useless as the degree of the conjugation $x \mapsto x^{3^{\frac{n+1}{2}}}$ is to high. It is an open problem how to evaluate such kind of character sums. It is conjectured that this sum is non-zero.

5 Further research

In this paper we gave a general family of low uniformity which is bijective for $p \equiv 3 \bmod 4$. If $p = 3$ the family has uniformity of at most 4 and its inverse family has a simple and closed description. To compute the uniformity we made use of the multivariate method and showed that it is a universal tool to do so. The advantage of this approach is that it yields concrete paramterizations for the solutions of $\Delta_{d_n,1}\left(x - \frac{1}{2}\right) = a$. This is particularly useful if one

wants to compute the cross-correlation. An example is the proof given in [6] for ternary decimations of Welch and Niho type. Many families of low uniformity can be represented as in this paper by power mappings, where a conjugation of the form $p^{\frac{n+1}{2}}$ or $p^{\frac{n}{2}}$ is involved as well as the quadratic character χ_{p^n}. Computing good upper bounds the uniformity by the multivariate method is often an almost routine matter whereas determining the exact uniformity leads to the problem of showing that a character sum as given in (26) is nonzero. Standard techniques to do so make use of the Weil bound. This is very often not applicable for the character sums arising from that kind of power mappings. An approach to show that such kind of character sums are non-zero would be an enormous step forward in the theory of computing the uniformity of power mappings in odd characteristic. Another approach to compute the exact uniformity for the mappings given in theorem 2.2 could be to analyze if the technique to treat the Δ-mapping in the proof given in [6] for the ternary decimations of Welch and Niho type can be adapted. This proof made extensively use of the fact that these decimations yield permutations x^{d_n} with a simple description for the inverse.

For applications in cryptography it is also of interest to analyze if the mappings presented here are strong against linear cryptanalysis and related attacks when employed in a block- or stream cipher. To compute the cross-correlation would be a fruitful next step in this direction.

Acknowledgments Open Access funding provided by Projekt DEAL.

References

1. Berndt, B., Evans, R., Williams, K.: Gauss and Jacobi Sums, vol. 21. Wiley-Interscience Publication
2. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Crypt. **15**(2), 125–156 (1998)
3. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties and Algorithms. Undergraduate Texts in Mathematics, 2nd edn. Springer (1997)
4. Dembowski, P., Ostrom, T.: Planes of order n with collineation group of order n^2. Math. Z. **103**, 239–258 (1968)
5. Dempwollf, U.: CCZ-Equivalence of Power Functions. Designs, Codes and Cryptography. Issue 03/2018, pp. 665–692. Springer. https://doi.org/10.1007/s10623-017-0350-8 (2018)
6. Dobbertin, H., Helleseth, T., Kumar, V., Martinsen, H.: Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type. Inform. Theory IEEE Trans. Inf. Theory **47**(4), 1473–1481 (2001). https://doi.org/10.1109/18.923728
7. Dobbertin, H., Mills, D., Müller, E.N., Pott, A., Willems, W.: APN functions in odd characteristic. Discret. Math. **267**, 95–112 (2003)
8. Felke, P.: A systematic approach with the multi-variate method over finite fields of odd characteristic. PhD Dissertation Ruhr-Universität Bochum (2005)
9. Helleseth, T., Rong, C., Sandberg, D.: New families of almost perfect nonlinear power functions. IEEE Trans. Inform. Theory **45**, 475–485 (1999)
10. Helleseth, T., Sandberg, D.: Some power functions with low differential uniformity. AAECC **8**, 363–370 (1997)

11. IOTA Cryptocurrency: https://cryptobriefing.com/iota-new-hash-function/
12. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory.Graduate Texts in Mathematics, pp. 84. Springer
13. Lidl, R., Niederreiter, H. Finite Fields. Encyclopedia of Mathematics and its Applications, 2nd edn., vol. 20. Cambridge University Press, Cambridge (1997)
14. Leducq, E.: New families of APN functions in characteristic 3 or 5.Arithmetic, Geometry. Cryptography and Coding Theory: 13th Conference, Contemporary Mathematics, AMS, 2011, Theorie des Fonctions Numeriques Simplement Periodiques. Amer. J. Math. **1**(3), 115–123 (1878)
15. Zha, Z., Wang, X.: Power functions with low uniformity on odd characteristic finite fields. Sci. China Math. **53**(8), 1931–1940 (2010). https://doi.org/10.1007/s11425-010-3149-x