LETTER

New Ternary Power Mapping with Differential Uniformity $\Delta_f \leq 3$ and Related Optimal Cyclic Codes

Haode YAN[†a)], *Member and* Dongchun HAN[†b)], *Nonmember*

SUMMARY In this letter, the differential uniformity of power function $f(x) = x^e$ over GF(3^m) is studied, where $m \geq 3$ is an odd integer and $e = \frac{3^m-3}{4}$. It is shown that $\Delta_f \leq 3$ and the power function is not CCZ-equivalent to the known ones. Moreover, we consider a family of ternary cyclic code $C_{(1,e)}$, which is generated by $m_\omega(x)m_{\omega^e}(x)$. Herein, ω is a primitive element of GF(3^m), $m_\omega(x)$ and $m_{\omega^e}(x)$ are minimal polynomials of ω and ω^e, respectively. The parameters of this family of cyclic codes are determined. It turns out that $C_{(1,e)}$ is optimal with respect to the Sphere Packing bound.

key words: *power mapping, differential uniformity, cyclic code*

1. Introduction

Let $F(x)$ be a function from GF(p^n) into GF(p^n), where p is a prime number. The *derivative* of $F(x)$ with respect to a given $a \in$ GF(p^n) is the function $\mathbb{D}_aF(x)$ from GF(p^n) to GF(p^n) defined by

$$\mathbb{D}_aF(x) = F(x+a) - F(x), \quad \forall\, x \in \mathrm{GF}(p^n).$$

For any $a \in \mathrm{GF}(p^n)^* := \mathrm{GF}(p^n) \setminus \{0\}$ and $b \in$ GF(p^n), we denote

$$\Delta_F(a,b) = \#\{x \in \mathrm{GF}(p^n) | \, \mathbb{D}_aF(x) = b\}.$$

The *differential uniformity* of F is defined as

$$\Delta_F = \max_{a \neq 0,\ b \in \mathrm{GF}(p^n)} \Delta_F(a,b).$$

Then F is said to be *differentially k-uniform* if $\Delta_F = k$. In particular, F is called perfect nonlinear (PN) when $k = 1$, and almost perfect nonlinear when $k = 2$. Note that PN functions only exist over finite fields with odd characteristic. When $F(x)$ is a power mapping, i.e., $F(x) = x^d$ for some positive integer d, then $\Delta_F(a,b) = \Delta_F(1, b/a^d)$ for all $a \in \mathrm{GF}(p^n)^*$ and $b \in$ GF(p^n). Hence the differential characteristics of the power monomial F is completely determined by the values $\Delta_F(1,b)$ for all $b \in$ GF(p^n). The known PN or APN power mappings $F(x) = x^d$ readers can refer to [6], [8], [13]–[15], [18]–[20].

Differential uniformity is an important concept in cryptography as it quantifies the degree of security of the *Substitution box* used in the cipher with respect to differential attacks [1]. Power functions with low differential uniformity, i.e., monomial functions of the form x^d serve as good candidates for the design of S-boxes not only because of their strong resistance to differential attacks but also for the usually low implementation cost in hardware environment. Power functions with high differential uniformity may introduce some unsuitable weaknesses within a cipher [2], [3], [7], [16]. Therefore it is worthwhile to study power functions with low differential uniformity as it provides better resistance towards differential cryptanalysis. For example, the AES (advanced encryption standard) employs a differentially 4-uniform power function which is EA-equivalent to the inverse function $x \mapsto x^{-1}$ over GF(2^n), where n is an even integer.

In addition to their applications in cryptography, functions with low differential uniformity are also useful in sequences, coding theory, and combinatorial designs. In sequences, they permit to construct sequences with optimal Hamming or inner-product correlation (c.f., [11], [17]). In coding theory, they are used to obtain cyclic codes or linear codes with excellent parameters (c.f., [4], [5]). It turns out that functions with low differential uniformity correspond to certain combinatorial designs (c.f., [6], [12]). Thus the study of functions with low differential uniformity could lead to new problems in combinatorics.

Although PN and APN power mappings are important and interesting, it seems hard to find new infinite families of PN and APN power mappings which are not equivalent to the known ones. Recently, only few results obtained. It is worth finding differentially 3-uniform power mappings. In this letter, we consider power function $f(x) = x^e$ over GF(3^m), where $m \geq 3$ is an odd integer and $e = \frac{3^m-3}{4}$. It is proved that $\Delta_f \leq 3$. However, we cannot determine whether the equality holds. Numerical results show that $f(x) = x^e$ is differentially 3-uniform when $m = 3, 5, \cdots, 15$. We leave this as a conjecture and invite the reader to settle it. We also considered the CCZ-equivalence. Thanks to a recent result proposed in [9], it is easy to check that our power mapping is not CCZ-equivalent to the known ones. Moreover, we use this power mapping to construct cyclic codes by using a generic construction, which is presented in [4], [10]. A family of optimal ternary cyclic codes are obtained. The rest of this letter is organized as follows. Some useful lemmas are given in Sect. 2. In Sect. 3, we prove the differential uniformity of $f(x) = x^e$ is not more than 3. Related cyclic codes are introduced in Sect. 4. Section 5 concludes the letter.

Manuscript received January 16, 2019.
Manuscript revised February 25, 2019.

[†]The authors are with School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China.
a) E-mail: hdyan@swjtu.edu.cn
b) E-mail: han-qingfeng@163.com (Corresponding author)

DOI: 10.1587/transfun.E102.A.849

2. Preliminaries

In this section, we will introduce some lemmas. We begin this section by fixing some notation which will be used throughout this letter unless otherwise stated.

- $m \geq 3$ is an odd integer and $e = \frac{3^m-3}{4}$ is even.
- We denote by SQ (resp. NSQ) the set of nonzero square (resp. nonzero nonsquare) elements in $\mathrm{GF}(3^m)$. Particularly, $-1 \in$ NSQ.
- γ is a primitive element in $\mathrm{GF}(3^2)$ such that $\gamma^2+\gamma-1 = 0$.
- $\delta = \gamma^2$ such that $\delta^2 = -1$.

We have the following lemma.

Lemma 1. *Let $f(x)$ be a polynomial over* $\mathrm{GF}(3)$ *with degree* 4. *If $f(x)$ has no root in* $\mathrm{GF}(3)$*, then it has no root in* $\mathrm{GF}(3^m)$.

Proof. Let x_0 be a root of $f(x)$. Since $f(x)$ has no root in $\mathrm{GF}(3)$, $f(x)$ is irreducible over $\mathrm{GF}(3)$ or $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are irreducible over $\mathrm{GF}(3)$ with degree 2. Then $x_0 \in \mathrm{GF}(3^4)$ or $x_0 \in \mathrm{GF}(3^2)$. Hence $x_0 \notin \mathrm{GF}(3^m)$ since m is odd. □

The following lemma shows the solutions of some equations over $\mathrm{GF}(3^m)$ and it will employed later.

Lemma 2. *Each of the following four equations has unique solution in* $\mathrm{GF}(3^m)$.

(i) $(x+1)^e - x^e = 0$.

(ii) $(x+1)^e - x^e - 1 = 0$.

(iii) $(x+1)^e - x^e + 1 = 0$.

(iv) $(x+1)^e + x^e + 1 = 0$.

Proof. It is easy to prove (i). Since $x \neq 0$, $(\frac{x+1}{x})^e = 1$. Then $\frac{x+1}{x} = \pm 1$ since $\gcd(e, 3^m-1) = 2$. Then $x = 1$ is the unique solution.

Next we prove (ii). Obviously, $x = 0$ is a solution of $(x+1)^e - x^e - 1 = 0$ and $x = -1$ is not. When $x \neq 0, -1$, we distinguish among the following four cases to determine all the solutions of $(x+1)^e - x^e - 1 = 0$ in $\mathrm{GF}(3^m)$.

Case 1. $x+1 \in$ SQ, $x \in$ SQ. We can write $x = u^2$ for some $u \in$ SQ since $-1 \in$ NSQ. Then $(u^2+1)^e = (u^2)^e + 1 = u^{-1} + 1$. Take the square of both sides of this identity, we can deduce

$$u^4 - u^3 + u^2 - u + 1 = 0 \tag{1}$$

since $x+1 \in$ SQ. By Lemma 1, (1) has no solution in $\mathrm{GF}(3^m)$.

Case 2. $x+1 \in$ NSQ, $x \in$ SQ. We can also write $x = u^2$ for some $u \in$ SQ. Similarly, we obtain $(u-1)^4 = 0$, which implies $u = 1$. Then $x = 1$, it is impossible.

Case 3. $x+1 \in$ SQ, $x \in$ NSQ. We can write $x = -u^2$ for some $u \in$ SQ. We obtain $u^4 - u^3 + u^2 + u - 1 = 0$. It has no solution in $\mathrm{GF}(3^m)$ by Lemma 1.

Case 4. $x+1 \in$ NSQ, $x \in$ NSQ. We can also write $x = -u^2$ for some $u \in$ SQ. We obtain $u^4 - u^3 - u^2 + u - 1 = 0$. It has no solution in $\mathrm{GF}(3^m)$ by Lemma 1.

The discussion above finishes the proof of (ii). The proofs of (iii) and (iv) are similar with that of (ii) and we omit them. The unique solutions of (iii) and (iv) are $x = -1$ and $x = 1$, respectively. □

We also need the following lemmas on the solutions in $\mathrm{GF}(3^m)$ for fixed $b_0 \in \mathrm{GF}(3^m) \setminus \mathrm{GF}(3)$.

Lemma 3. *Let $b_0 \in$* $\mathrm{GF}(3^m) \setminus \mathrm{GF}(3)$. *If $b_0 \in SQ$ (resp. NSQ), then the equation*

$$\frac{x^3}{x^4-1} = b_0 \tag{2}$$

has at most one solution in NSQ (resp. SQ).

Proof. We only prove the case that $b_0 \in$ SQ. If (2) has solutions in NSQ, let $\theta \in$ NSQ be a solution of (2). If there exists $\varphi \neq \theta$ in NSQ such that (2) holds, then $\theta\varphi \in$ SQ. Moreover, $\frac{\theta^3}{\theta^4-1} = \frac{\varphi^3}{\varphi^4-1}$, that is,

$$(\theta\varphi)^3 = -(\theta-\varphi)^2.$$

It is a contradiction. Then the number of solutions of (2) in NSQ is at most 1. □

Lemma 4. *Let $b_0 \in$* $\mathrm{GF}(3^{2m})^*$. *If $\theta \in$* $\mathrm{GF}(3^{2m})^*$ *is a solution of*

$$\frac{x^3+\delta x}{x^4-1} = b_0, \tag{3}$$

then the solutions of (3) are $\theta, \delta\theta^{-1}, -\gamma^3\frac{\theta+\gamma^3}{\theta-\gamma^3}$ and $\gamma^3\frac{\theta-\gamma^3}{\theta+\gamma^3}$.

Proof. Suppose $\varphi \neq \theta$ is a solution of (3), then $\frac{\theta^3+\delta\theta}{\theta^4-1} = \frac{\varphi^3+\delta\varphi}{\varphi^4-1}$. That is,

$$(\varphi-\theta)(\theta\varphi-\delta)((\theta\varphi-\delta)+\gamma^3(\varphi-\theta))$$
$$((\theta\varphi-\delta)-\gamma^3(\varphi-\theta)) = 0.$$

$\theta \neq 0, \pm\gamma^3$ since $b_0 \neq 0$. Then Lemma 4 follows. □

Similarly, we present the following lemma without proof.

Lemma 5. *Let $b_0 \in$* $\mathrm{GF}(3^{2m})^*$. *If $\theta \in$* $\mathrm{GF}(3^{2m})^*$ *is a solution of*

$$\frac{x^3-\delta x}{x^4-1} = b_0, \tag{4}$$

then the solutions of (4) are $\theta, -\delta\theta^{-1}, -\gamma\frac{\theta+\gamma}{\theta-\gamma}$ and $\gamma\frac{\theta-\gamma}{\theta+\gamma}$.

3. Ternary Power Mapping with Low Differential Uniformity

In this section, we introduce a class of ternary power mapping over $\mathrm{GF}(3^m)$ with low differential uniformity. The following is the main result of the present letter.

Theorem 1. *Let m be an odd integer, $e = \frac{3^m-3}{4}$. The power mapping $f(x) = x^e$ in* GF(3^m) *satisfies* $\Delta_f \leq 3$.

Proof. Consider the equation

$$(x+1)^e - x^e = b. \tag{5}$$

We should prove that the number of solutions of equation (5) is not more than 3 for any $b \in \mathrm{GF}(3^m)$. It was proved in Lemma 2 that (5) has unique solution when $b \in \mathrm{GF}(3)$. Then we consider fixed $b \in \mathrm{GF}(3^m) \setminus \mathrm{GF}(3)$, it is obvious that the solutions of (5) are in $\mathrm{GF}(3^m) \setminus \mathrm{GF}(3)$. Assume that x is a solution of (5), we distinguish among the following four cases.

Case I. $x + 1 \in \mathrm{SQ}$, $x \in \mathrm{SQ}$. In this case, we write $x + 1 = \alpha^2$ and $x = \beta^2$ for $\alpha, \beta \in \mathrm{SQ}$. Then $\alpha^2 - \beta^2 = 1$. Let $\theta = \alpha - \beta \in \mathrm{GF}(3^m)^*$, $\alpha + \beta = \theta^{-1}$. Then $\alpha = -\theta - \theta^{-1}$ and $\beta = \theta - \theta^{-1}$. Note that $x = \beta^2 = (\theta - \theta^{-1})^2$, x is uniquely determined by θ. In order to investigate the number of solution of (5) in this case, it is sufficient to find the number of θ satisfy (6) for the fixed b. Moreover, $b = \alpha^{2e} - \beta^{2e} = \alpha^{-1} - \beta^{-1}$, we have

$$b = \frac{\theta^3}{\theta^4 - 1}. \tag{6}$$

Notice that $\alpha = -\frac{\theta^2+1}{\theta}$ and $\beta = \frac{\theta^2-1}{\theta}$ are both in SQ, then we have $\theta^4 - 1 \in \mathrm{NSQ}$, which implies $b\theta \in \mathrm{NSQ}$. By Lemma 3, there are at most one $\theta \in \mathrm{GF}(3^m)^*$ satisfies (6). Then the number of solutions in Case I is at most one.

Case II. $x + 1 \in \mathrm{NSQ}$, $x \in \mathrm{NSQ}$. In this case, we write $x + 1 = -\alpha^2$ and $x = -\beta^2$ for $\alpha, \beta \in \mathrm{SQ}$. Then $\alpha^2 - \beta^2 = -1$ and $b = \alpha^{2e} - \beta^{2e} = \alpha^{-1} - \beta^{-1}$. Let $\theta = \alpha - \beta \in \mathrm{GF}(3^m)^*$, $\alpha + \beta = -\theta^{-1}$. Then $\alpha = -\theta + \theta^{-1}$ and $\beta = \theta + \theta^{-1}$. $x = -\beta^2$ is uniquely determined by θ. In this case, we also have $b = \frac{\theta^3}{\theta^4-1}$. Notice $\alpha = -\frac{\theta^2-1}{\theta}$ and $\beta = \frac{\theta^2+1}{\theta}$ are both elements in SQ, then we still have $\theta^4 - 1 \in \mathrm{NSQ}$ and then $b\theta \in \mathrm{NSQ}$. It follows from Lemma 3 that the number of solutions in Case II is at most one.

In both Cases I and II, $\theta^4 - 1 \in \mathrm{NSQ}$, and θ satisfies (6). By Lemma 3, if there exists such θ, it is the unique one. Note that θ cannot satisfy that all $-\frac{\theta^2+1}{\theta}, \frac{\theta^2-1}{\theta}, -\frac{\theta^2-1}{\theta}, \frac{\theta^2+1}{\theta} \in$ SQ. This implies (5) cannot have solutions in Cases I and II simultaneously. The number of solutions in both Cases I and II is at most one.

Case III. $x + 1 \in \mathrm{SQ}$, $x \in \mathrm{NSQ}$. In this case, we write $x+1 = \alpha^2$ and $x = -\beta^2$ for $\alpha, \beta \in \mathrm{SQ}$. Then $\alpha^2 + \beta^2 = 1$ and $b = \alpha^{2e} - \beta^{2e} = \alpha^{-1} - \beta^{-1}$. Let $\theta = \alpha - \delta\beta \in \mathrm{GF}(3^{2m})^*$, $\alpha + \delta\beta = \theta^{-1}$. Then $\alpha = -\theta - \theta^{-1}$, $\beta = -\delta(\theta - \theta^{-1}) \in \mathrm{GF}(3^m)$, we can find that θ satisfies $\theta^{3^m+1} = 1$. In this case, we have

$$b = -(1+\delta)\frac{\theta^3 + \delta\theta}{\theta^4 - 1}. \tag{7}$$

By Lemma 4, the other solutions of (7) are $\delta\theta^{-1}$, $-\gamma^3\frac{\theta+\gamma^3}{\theta-\gamma^3}$ and $\gamma^3\frac{\theta-\gamma^3}{\theta+\gamma^3}$. Note that $\alpha = -\theta - \theta^{-1}$, $\beta = -\delta(\theta - \theta^{-1})$ and $\alpha\beta = \delta(\theta^2 - \theta^{-2}) = \delta\frac{\theta^4-1}{\theta^2}$ are all in SQ. We can verify that

$$-(\delta\theta^{-1}) - (\delta\theta^{-1})^{-1} = \delta(\theta - \theta^{-1}) \in \mathrm{NSQ},$$

then $\delta\theta^{-1}$ cannot correspond to a solution of (5). Moreover,

$$\delta((-\gamma^3\frac{\theta+\gamma^3}{\theta-\gamma^3})^2 - (-\gamma^3\frac{\theta+\gamma^3}{\theta-\gamma^3})^{-2})$$

$$= \delta((\gamma^3\frac{\theta-\gamma^3}{\theta+\gamma^3})^2 - (\gamma^3\frac{\theta-\gamma^3}{\theta+\gamma^3})^{-2}) = -\frac{\theta^4-1}{(\theta^2+\delta)^2}.$$

If $-\frac{\theta^4-1}{(\theta^2+\delta)^2} \in \mathrm{SQ}$, then $\frac{\delta\theta^2}{(\theta^2+\delta)^2} \in \mathrm{SQ}$ since $\delta\frac{\theta^4-1}{\theta^2} \in \mathrm{SQ}$, which implies $\frac{\gamma\theta}{\theta^2+\delta} \in \mathrm{GF}(3^m)$. Then $\frac{\gamma\theta}{\theta^2+\delta} = (\frac{\gamma\theta}{\theta^2+\delta})^{3^m}$. Combining with $\theta^{3^m+1} = 1$ and $\gamma^{3^m} = \gamma^3$, we have $\theta^2 = -\delta$, which is a contradiction. That means $-\gamma^3\frac{\theta+\gamma^3}{\theta-\gamma^3}$ and $\gamma^3\frac{\theta-\gamma^3}{\theta+\gamma^3}$ cannot correspond to a solution of (5). Then the solution of (5) in this case is at most one.

Case IV. $x + 1 \in \mathrm{NSQ}$, $x \in \mathrm{SQ}$. In this case, we write $x + 1 = -\alpha^2$ and $x = \beta^2$ for $\alpha, \beta \in \mathrm{SQ}$. Then $\alpha^2 + \beta^2 = -1$ and $b = \alpha^{2e} - \beta^{2e} = \alpha^{-1} - \beta^{-1}$. Let $\theta = \alpha - \delta\beta \in \mathrm{GF}(3^{2m})^*$, $\alpha + \delta\beta = -\theta^{-1}$. Then $\alpha = -\theta + \theta^{-1}$, $\beta = -\delta(\theta + \theta^{-1}) \in \mathrm{GF}(3^m)$, we can find that θ satisfies $\theta^{3^m+1} = -1$. In this case, we have

$$b = -(1+\delta)\frac{\theta^3 - \delta\theta}{\theta^4 - 1}. \tag{8}$$

By Lemma 5, the other solutions of (8) are $-\delta\theta^{-1}$, $-\gamma\frac{\theta+\gamma}{\theta-\gamma}$ and $\gamma\frac{\theta-\gamma}{\theta+\gamma}$. Similarly, it can be check that these three solutions cannot correspond to a solution of (5), the details are omitted.

Summarizing the discussion above completes the proof of Theorem 1. □

Although we proved that $\Delta_f \leq 3$, it seems difficult to determine that $\Delta_f = 3$. Numerical results show that $f(x) = x^e$ is differentially 3-uniform when $m = 3, 5, \cdots, 15$. We leave this as a conjecture. The reader is kindly invited to work out it.

Conjecture. Let m be an odd integer, $e = \frac{3^m-3}{4}$. The differential uniformity of power mapping $f(x) = x^e$ over GF(3^m) is 3.

4. Optimal Ternary Cyclic Codes Form $f(x) = x^e$

In this section, we introduce a generic construction of cyclic codes and then we use $f(x) = x^e$ to construct optimal ternary cyclic codes.

Let p be a prime and let $q = p^m$, where m is a positive integer. Let $m_{\omega^i}(x)$ denote the minimal polynomial of ω^i over GF(p). Consider the cyclic code of length $n = q-1$ over GF(p) with generator polynomial $m_\omega(x)m_{\omega^\ell}(x)$, denoted by $C_{(1,\ell)}$, where $1 < \ell < q-1$ such that ω and ω^ℓ are nonconjugate. For the ternary case, i.e. $p = 3$, the cyclic code $C_{(1,\ell)}$ was widely studied, see [4], [10]. We are mostly interested in the case that the degree of $m_{\omega^\ell}(x)$ is equal to

m. This makes the code $C_{(1,\ell)}$ has dimension $3^m - 1 - 2m$. According to the sphere packing bound, it is obtained that the maximal minimum distance of a code with length $3^m - 1$ and dimension $3^m - 1 - 2m$ is 4. A natural question one would ask is when the code $C_{(1,\ell)}$ has optimal minimum distance. The following theorem shows the sufficient and necessary condition.

Theorem 2 ([10], Theorem 4.1)**.** *Let ω and ω^ℓ are nonconjugate and $\deg(m_{\omega^\ell}(x)) = m$. The cyclic code $C_{(1,\ell)}$ over $\mathrm{GF}(3^m)$ has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$ if and only if the following conditions are satisfied:*

C1: ℓ is even.

C2: the equation $(x + 1)^\ell + x^\ell + 1 = 0$ has the only solution $x = 1$ in $\mathrm{GF}(3^m)^*$; and

C3: the equation $(x + 1)^\ell - x^\ell - 1 = 0$ has the only solution $x = 0$ in $\mathrm{GF}(3^m)$.

Now we use the power mapping with low differential uniformity to construct cyclic codes. We choose ℓ equals to e, the power of $f(x)$, which we studied in Sect. 3. When $e = \frac{3^m-3}{4}$ and $m \geq 3$ is an odd integer, it is easy to verify that ω and ω^e are nonconjugate and $\deg(m_{\omega^e}(x)) = m$. The conditions in Theorem 2 can be verified by Lemma 2, a class of optimal cyclic codes are obtained.

Theorem 3. *Let $m \geq 3$ be an odd integer and $e = \frac{3^m-3}{4}$. The ternary cyclic code $C_{(1,e)}$ is an optimal cyclic code with parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.*

The following examples from the Magma Program confirm Theorem 3.

Example 1. Let $m = 5$ and ω be a generator of $\mathrm{GF}(3^m)^*$ with minimal polynomial $x^5 + 2x + 1$. Then the code $C_{(1,e)}$ is an optimal ternary cyclic code with generator polynomial $x^{10}+2x^8+x^7+x^4+x^3+2x+2$ and parameters $[242, 232, 4]$.

Example 2. Let $m = 7$ and ω be a generator of $\mathrm{GF}(3^m)^*$ with minimal polynomial $x^7 + 2x + 1$. Then the code $C_{(1,e)}$ is an optimal ternary cyclic code with generator polynomial $x^{14}+2x^{13}+2x^{12}+2x^{10}+x^8+x^7+2x^6+2x^4+x^3+2x^2+x+2$ and parameters $[2186, 2172, 4]$.

Example 3. Let $m = 9$ and ω be a generator of $\mathrm{GF}(3^m)^*$ with minimal polynomial $x^9 + 2x^3 + 2x^2 + x + 1$. Then the code $C_{(1,e)}$ is an optimal ternary cyclic code with generator polynomial $x^{18}+x^{17}+2x^{15}+2x^{13}+2x^{12}+2x^{11}+2x^{10}+2x^9+2x^8+x^5+2x^4+x^2+x+2$ and parameters $[19682, 19664, 4]$.

5. Concluding Remarks

In this letter, we provided a class of power function with low differential uniformity. More precisely, let $f(x) = x^e$ be a power function over $\mathrm{GF}(3^m)$, where $m \geq 3$ is an odd integer and $e = \frac{3^m-3}{4}$, it is proved that $\Delta_f \leq 3$. We conjectured that $\Delta_f = 3$ and invited readers to settle it. The related codes are also studied. We use this power e to construct cyclic codes by using a generic construction. A family of ternary optimal cyclic codes are obtained. It is worth finding more infinite families of power functions with low differential uniformity.

Acknowledgments

The author sincerely thanks Professor Tor Helleseth for his useful comments which improve the quality of this letter. Yan's research was supported by the National Natural Science Foundation of China under Grant 11801468 and the Fundamental Research Funds for the Central Universities of China under Grant 2682018CX61. Han's research was supported by the National Natural Science Foundation of China under Grant 11601448 and the Fundamental Research Funds for the Central Universities of China under Grant 2682016CX121.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," J. Cryptol., vol.4, no.1, pp.3–72, 1991.

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," Int. J. Inf. Coding Theory, vol.1, no.2, pp.149–170, 2010.

[3] A. Canteaut and M. Videau, "Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis," Advances in Cryptology – EUROCRYPT 2002, Lecture Notes in Comput. Sci., vol.2332, pp.518–533, Springer, Berlin, 2002.

[4] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," Des. Codes Cryptogr., vol.15, no.2, pp.125–156, 1998.

[5] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," IEEE Trans. Inf. Theory, vol.51, no.6, pp.2089–2102, 2005.

[6] R.S. Coulter and R.W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," Des. Codes Cryptogr., vol.10, no.2, pp.167–184, 1997.

[7] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," Advances in Cryptology – ASIACRYPT 2002, Lecture Notes in Comput. Sci., vol.2501, pp.267–287, Springer, Berlin, 2002.

[8] P. Dembowski and T.G. Ostrom, "Planes of order n with collineation groups of order n^2," Math. Z., vol.103, no.3, pp.239–258, 1968.

[9] U. Dempwolff, "CCZ equivalence of power functions," Des. Codes Cryptogr., vol.86, no.3, pp.665–692, 2018.

[10] C. Ding and T. Helleseth, "Optimal ternary cyclic codes from monomials," IEEE Trans. Inf. Theory, vol.59, no.9, pp.5898–5904, 2013.

[11] C. Ding, M.J. Moisio, and J. Yuan, "Algebraic constructions of optimal frequency-hopping sequences," IEEE Trans. Inf. Theory, vol.53, no.7, pp.2606–2610, 2007.

[12] C. Ding and J. Yuan, "A family of skew Hadamard difference sets," J. Comb. Theory, Ser. A, vol.113, no.7, pp.1526–1535, 2006.

[13] H. Dobbertin, D. Mills, E.N. Muller, A. Pott, and W. Willems, "APN functions in odd chatacteristic," Discr. Math., vol.267, no.1-3, pp.95–112, 2003.

[14] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," IEEE Trans. Inf. Theory, vol.45, no.2, pp.475–485, 1999.

[15] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," Appl. Algebra Engrg. Comm. Comput., vol.8, no.5, pp.363–370, 1997.

[16] T. Jakobsen and L.R. Knudsen, "The interpolation attack on block ciphers," Fast Software Encryption – FSE 1997, Lecture Notes in Comput. Sci., vol.1267, pp.28–40, Springer, Berlin, 1997.

[17] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inf. Theory, vol.37, no.3, pp.603–616, May 1991.

[18] E. Leducq, “New families of APN functions in characteristic 3 or 5,” Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol.574, pp.115–123, AMS 2012.

[19] Z. Zha and X, Wang, “Power functions with low uniformity on odd characteristic finite fields,” Sci. China Math., vol.53, no.8, pp.1931–1940, 2010.

[20] Z. Zha and X. Wang, “Almost perfect nonlinear power functions in odd characteristic,” IEEE Trans. Inf. Theory, vol.57, no.7, pp.4826–4832, 2011.