Noname manuscript No.
(will be inserted by the editor)

Constructing differential 4-uniform permutations from know ones

Yuyin Yu · Mingsheng Wang · Yongqiang Li

Received: date / Accepted: date

Abstract It is observed that exchanging two values of a function over $\mathbb{F}_{2^n}$, its differential uniformity and nonlinearity change only a little. Using this idea, we find permutations of differential 4-uniform over $\mathbb{F}_{2^6}$ whose number of the pairs of input and output differences with differential 4-uniform is 54, less than 63, which provides a solution for an open problem proposed by Berger et al. [1]. Moreover, for the inverse function over $\mathbb{F}_{2^n}$ (n even), various possible differential uniformities are completely determined after its two values are exchanged. As a consequence, we get some highly nonlinear permutations with differential uniformity 4 which are CCZ-inequivalent to the inverse function on $\mathbb{F}_{2^n}$.

Keywords vectorial boolean function · differential uniformity · nonlinearity · CCZ-equivalence · almost perfect nonlinear (APN)

Mathematics Subject Classification (2000) 06E30 · 11T06 · 94A60

1 Introduction

Differential uniformity and nonlinearity are two main factors when we consider the cryptographic properties of a function, we expect to find functions with low differential uniformity and high nonlinearity, because such functions can provide good resistance to differential and linear attack. As to differential property, we know that APN functions

Y. Yu · M. Wang · Y. Li
The State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing 100190, PO Box 8718, China

M. Wang (Corresponding author)
E-mail: mingsheng_wang@yahoo.com.cn

Y. Yu · Y. Li
Graduate School of Chinese Academy of Sciences, Beijing 100190, China
E-mail: yuyuyin@163.com ; liyongqiang@is.iscas.ac.cn

provide optimal resistance to differential attack. There has been much recent research and progress on APN functions (See [5], [6], [3], [4], [7], [12]). However, at present there are no known APN permutations defined on even degree fields greater than 6, so it still remains an important open problem whether APN permutations exist on $\mathbb{F}_{2^n}$ with n even and greater than 6. There is no better choice, so the AES (advanced encryption standard) chose the inverse function, which is a differential 4 uniform function. As a matter of fact, even finding differential 4 uniform permutation functions with high nonlinearity on even degree fields are a very big challenge. There is some recent work in this field (See [3], [7]). In view of these reasons, in [3], Bracken and Leander listed an open problem:

Problem 1 Find more highly nonlinear permutations of even degree fields with differential uniformity of 4.

This paper is a response to this open problem. With the method proposed in this paper, we can construct many highly nonlinear permutations with differential 4-uniform on the field $\mathbb{F}_{2^{2m}}$ $(m \geq 2)$ from the inverse function, and the new constructed functions are not CCZ-equivalent to the original function because most of the time they have different nonlinearity. The polynomial representation of new functions are very complex (See the Appendix for an example over $\mathbb{F}_{2^8}$), they are very different from the inverse function.

Berger et al. [1] investigated some open problems on APN functions over $\mathbb{F}_{2^n}$. As to permutations of differential uniformity 4, they listed an open problems as follows:

Problem 2 Find a permutation F on $\mathbb{F}_{2^n}$, n even, with components $f_\lambda, \lambda \in \mathbb{F}_{2^n}^*$, such that $\delta(F) = 4$ (See Definition 1) and

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A2^{n+3} \tag{1}$$

for some integer $A < 2^n - 1$, where $A = \#\{(a,b) \big| \ \delta_F(a,b) = 4,\ a \neq 0\}$.

According to [1], Equation (1) is an identical equation when $\delta(F) = 4$. So the problem is to find a permutation F on $\mathbb{F}_{2^n}$ with $A < 2^n - 1$ under the condition of $\delta(F) = 4$. In this paper, we indeed find such permutations, we will give a detailed description about such permutations in Sect. 3.2.

When we consider the properties of a function, we usually use the polynomial form to represent it. However, when we make some changes on the polynomial, then most values of the function will become different, so the properties of the new function may become very different from the original one. In this paper, we study the differential property of the function over $\mathbb{F}_{2^n}$ (n even), which is obtained from a given function through exchanging its two function values. The advantage of this method is that functions obtained in this way have very different forms but have very similar properties, so it might be useful in the design of cryptographic algorithms. The same method has appeared in [15], Fuller called this method "2-step tweaking" (See Sect. 6.4.1 of [15]), so this is not a new method. But in [15], Fuller focused on the linear redundancy of the new constructed functions, while we focus on the differential and nonlinear properties of the new constructed functions. Moreover, we use this method to consider some specific functions, for example, the inverse function, and we get many new results.

The paper is organized as follows. In Sect.2, we provide some necessary preliminaries, in Sect. 3, we introduce some basic properties and applications of our method, in Sect. 4, we give a detailed description about how to construct differential 4 uniform from the inverse function.

2 Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. Let $\mathbb{F}_{2^m}$ be a subfield of $\mathbb{F}_{2^n}$. $\mathrm{Tr}_{2^n/2^m}$ denotes the relative trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. Tr denotes the absolute trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

We introduce some basic concepts needed in this paper. Firstly, let's recall the following definition related to the resistance to differential cryptanalysis [17].

Definition 1 Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. For any a and b in $\mathbb{F}_{2^n}$, we denote

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

where $\#E$ is the cardinality of the set E. Then, we have

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

We can say that F is differential $\delta(F)$-uniform and the function for which equality holds is said to be almost perfect nonlinear(APN).

Definition 2 Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. The linear combinations of the coordinates of F are the Boolean functions:

$$f_\lambda : x \in \mathbb{F}_{2^n} \mapsto \mathrm{Tr}(\lambda F(x)), \quad \lambda \in \mathbb{F}_{2^n},$$

where f_0 is the null function. The functions f_λ are called the components of F.

For a Boolean function f on $\mathbb{F}_{2^n}$, we denote by $\mathscr{F}(f)$ the following value related to the Fourier transform of f:

$$\mathscr{F}(f) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)}.$$

Definition 3 Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. The nonlinearity of F is defined as

$$\mathcal{N}(F) = 2^{n-1} - \frac{1}{2} max_{a\neq 0,\, b\in \mathbb{F}_{2^n}} |\Lambda_F(a,b)|,$$

where $\Lambda_F(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(aF(x)+bx)}$.

The proof of the following equation can be found in [8].

Definition 4 Sum-of-square indicator of a Boolean function f is defined by

$$\nu(f) = \sum_{a\in\mathbb{F}_{2^n}} \mathscr{F}^2(f(a+x)+f(x)) = 2^{-n} \sum_{a\in\mathbb{F}_{2^n}} \mathscr{F}^4(f+\varphi_a),$$

where $\varphi_a(x) = \mathrm{Tr}(ax)$.

In this paper, we will use the following result [16]:

Lemma 1 *The equation $x^2+x+c=0$ has a solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(c)=0$.*

3 Basic properties and applications

3.1 Properties

When we do a few changes on the output values of a function, some properties of the function will not change too much. In this subsection, we will give a detailed description of such properties.

Proposition 1 *Let F, G be two functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ such that:*

$$\begin{cases} G(p_1) \neq F(p_1),\, p_1 \in \mathbb{F}_{2^n}; \\ G(x) = F(x), \quad x \in \mathbb{F}_{2^n} \textit{ and } x \neq p_1. \end{cases}$$

Then

$$\delta(F) - 2 \leq \delta(G) \leq \delta(F) + 2, \textit{and}$$

$$\mathcal{N}(F) - 1 \leq \mathcal{N}(G) \leq \mathcal{N}(F) + 1.$$

Proof From the relations of F and G, it is easy to see that $\forall (a, b) \in (\mathbb{F}_{2^n}^{*} \times \mathbb{F}_{2^n})$,

$$\Delta_F(a, b) \subseteq \Delta_G(a, b) \cup \{p_1, p_1 + a\},$$

$$\text{and} \quad \Delta_G(a, b) \subseteq \Delta_F(a, b) \cup \{p_1, p_1 + a\},$$

which imply the first part of this proposition. Now let's consider the second part of this proposition. $\forall (a, b) \in (\mathbb{F}_{2^n}^{*} \times \mathbb{F}_{2^n})$, let

$$\Lambda_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(aF(x)+bx)},$$

$$\Lambda_G(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(aG(x)+bx)}.$$

By the definition of G, we deduce that

$$|\Lambda_G(a, b) - \Lambda_F(a, b)| = |(-1)^{\mathrm{Tr}(aG(p_1)+bp_1)} - (-1)^{\mathrm{Tr}(aF(p_1)+bp_1)}| \leq 2. \tag{2}$$

From Definition 3 and Relation (2), we deduce that

$$\mathcal{N}(F) - 1 \leq \mathcal{N}(G) \leq \mathcal{N}(F) + 1.$$

□

This proposition tells us that if we change only one output value of a function, the differential and nonlinear properties of the function will change only a little, avalanche will not happen. This is really a good property which can be used to find new good functions from known ones, we will give some examples in the following subsection. But for now, let's have a look at the original idea of this paper.

Proposition 2 *Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. Define a new function G as follows:*

$$\begin{cases} G(p_1) = F(p_2),\ p_1, p_2 \in \mathbb{F}_{2^n} \text{ and } p_1 \neq p_2; \\ G(p_2) = F(p_1); \\ G(x) = F(x), \quad x \in \mathbb{F}_{2^n} \text{ and } x \neq p_1, p_2. \end{cases}$$

Then $\forall a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$, $\Delta_G(a,b) \subseteq \Delta_F(a,b) \bigcup \{p_1, p_1 + a, p_2, p_2 + a\}$, *and*

$$\delta(F) - 4 \leq \delta(G) \leq \delta(F) + 4,$$

$$\mathcal{N}(F) - 2 \leq \mathcal{N}(G) \leq \mathcal{N}(F) + 2.$$

Proof It is easy to see that Proposition 2 is just a corollary of Proposition 1. □

Especially, when F is an APN function, we have the following result:

Proposition 3 *Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$, define a new function G as follows:*

$$\begin{cases} G(p_1) = F(p_2),\ p_1, p_2 \in \mathbb{F}_{2^n} \text{ and } p_1 \neq p_2; \\ G(p_2) = F(p_1); \\ G(x) = F(x), \quad x \in \mathbb{F}_{2^n} \text{ and } x \neq p_1, p_2. \end{cases}$$

If $\delta(F) = 2$, *then*

$$\delta(G) \in \{2, 4\}.$$

Proof By Proposition 2, $2 \leq \delta(G) \leq 6$, we will prove $\delta(G) \neq 6$ in the following. Assume $\delta(G) = 6$. Then for some $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$,

$$\Delta_G(a,b) = \{x_1, x_1 + a, x_2, x_2 + a, x_3, x_3 + a\},$$

and the elements in $\Delta_G(a,b)$ are different from each other. By Proposition 2, we have

$$\Delta_G(a,b) \subseteq \Delta_F(a,b) \cup \{p_1, p_1 + a, p_2, p_2 + a\}. \tag{3}$$

We know that $\delta_F(a,b) = 2$ because F is an APN. Then there must be

$$|\Delta_F(a,b) \cup \{p_1, p_1 + a, p_2, p_2 + a\}| \leq 6 = \delta_G(a,b). \tag{4}$$

From (3) and (4) we conclude that

$$\Delta_G(a,b) = \Delta_F(a,b) \cup \{p_1, p_1 + a, p_2, p_2 + a\},$$

which implies

$$\{p_1, p_1 + a, p_2, p_2 + a\} \subseteq \Delta_G(a,b).$$

So, without loss of generality, we can suppose

$$p_1 = x_1, p_2 = x_2.$$

Then we will have

$$\begin{cases} G(p_1 + a) + G(p_1) = b \\ G(p_2 + a) + G(p_2) = b, \end{cases}$$

that is

$$\begin{cases} F(p_1 + a) + F(p_2) = b \\ F(p_2 + a) + F(p_1) = b, \end{cases}$$

Table 1 Value Table of F

0	54	48	13	15	18	53	35	25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37	60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62	47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49	9	6	23	32	30	12	55	22

Table 2 Value Table of $F_{(0,1)}$

54	0	48	13	15	18	53	35	25	63	45	52	3	20	41	33
59	36	2	34	10	8	57	37	60	19	42	14	50	26	58	24
39	27	21	17	16	29	1	62	47	40	51	56	7	43	44	38
31	11	4	28	61	46	5	49	9	6	23	32	30	12	55	22

which is equal to

$$\begin{cases} F(p_1 + a) + F(p_1 + a + (a + p_1 + p_2)) = b \\ F(p_2 + a) + F(p_2 + a + (a + p_1 + p_2)) = b. \end{cases} \tag{5}$$

By (5), we deduce that the equation

$$F(x) + F(x + (a + p_1 + p_2)) = b$$

has four solutions, which is impossible because F is APN. So $\delta(G) \neq 6$, which implies the conclusion. $\square$

As a matter of fact, we never get differential 2-uniform functions when we do tests in $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^7}$. Perhaps Proposition 3 provides a way to construct differential 4-uniform functions from known APN functions, and this transformation will keep the permutation properties if the original function is a permutation.

3.2 Applications

We have introduced an open problem proposed by Berger et al. [1] in the introduction, here we give the details about what we have done to this problem. We specify this problem to $n = 6$. First we introduce an APN permutation on $\mathbb{F}_{2^6}$ found by Dillon [12] which is described by a value table (Table 1). We denote the function by F, which satisfies:

$$F(0) = 0, F(1) = 54, F(2) = 48 \cdots, F(15) = 33, F(16) = 59, \cdots, F(63) = 22.$$

According to Proposition 3, if we exchange $F(i)$ and $F(j)$ $(i \neq j)$, then we get a lot of new functions, denoted as $F_{(i,j)}$, which satisfies $\delta(F_{(i,j)}) \in \{2, 4\}$. It is plausible to expect that function $F_{(i,j)}$ will keep many properties of the original function F (See Proposition 2). Based on these considerations, we traverse the pairs of $(i, j) \in (\mathbb{Z}_{2^6} \times \mathbb{Z}_{2^6})$ $(i \neq j)$, and finally find some $A < 2^6 - 1$, which satisfies the requirements of Problem 2. We give an example as follows:

Example 1 Exchanging values of $F(0)$ and $F(1)$ to get a new function $F_{(0,1)}$, which is described in Table 2:

By means of a computer, $\delta(F_{(0,1)}) = 4$, and the corresponding parameter $A = 54 < 2^6 - 1$, so we have found an example of Problem 2.

In fact, 1176 examples are found when we traverse the pairs of $(i,j) \in (\mathbb{Z}_{2^6} \times \mathbb{Z}_{2^6})$ $(i < j)$, we will not list all of them here. According to our computation, the following conjecture seems to be true:

Conjecture 1 If F is an APN permutation on $\mathbb{F}_{2^n}$, n even, then $\exists (i,j) \in (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n})$ $(i < j)$, such that the function $F_{(i,j)}$ is a permutation on $\mathbb{F}_{2^n}$ with $\delta(F_{(i,j)}) = 4$, and for components $f_\lambda, \lambda \in \mathbb{F}_{2^n}^*$, we have

$$\sum_{\lambda \in \mathbb{F}_{2^n}^*} \nu(f_\lambda) = (2^n - 1)2^{2n+1} + A2^{n+3}$$

for some integer $A < 2^n - 1$, where $A = \#\{(a,b) \Big| \ \delta_F(a,b) = 4,\ a \neq 0\}$.

4 Constructing differential 4-uniform from the inverse function

In this section, we will give a detailed discussion about the inverse function with the above idea. First we recall a formal definition about the inverse function.

Definition 5 Define the inverse function I on $\mathbb{F}_{2^n}$ as follows:

$$I(x) = \begin{cases} 0, & x = 0 \\ x^{-1}, & x \neq 0. \end{cases}$$

In this paper, we only consider the case when n is even.
The following result is simple, but it plays an important role in our discussion, we emphasize it here as a lemma.

Lemma 2 *Let $n = 2m (m \geq 1)$, $d = \frac{1}{3}(2^n - 1)$, and g a primitive element in $\mathbb{F}_{2^n}$. Then*

$$g^{2d} + g^d + 1 = 0. \tag{6}$$

Proof Since g is a primitive element in $\mathbb{F}_{2^n}$, $g^d \neq 1$. Furthermore, $(g^{2d}+g^d+1)(g^d+1) = g^{3d} + 1 = 0$, we have $g^{2d} + g^d + 1 = 0$. $\square$

It is well known that $\delta(I) = 4$ when n is even [17], but there are something wrong in [17] when considering the case $\delta(I) = 4$, we correct the error in the original paper and restate this result as follows:

Lemma 3 *Let $n = 2m (m \geq 1)$, $d = \frac{1}{3}(2^n - 1)$, and g be a primitive element in $\mathbb{F}_{2^n}$, $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$. Then the following statements are equivalent:*
(1) $\delta_I(a,b) = 4$;
(2) $b = a^{-1}$;
(3) $\Delta_I(a,b) = \{0, a, ag^d, ag^{2d}\}$, where $ag^d + a = ag^{2d}$.

In [17], the author gave four solutions of $I(x) + I(x+a) = a^{-1}$ as $\Delta_I(a, a^{-1}) = \{0, a, a^{1+d}, a^{1+2d}\}$. The result is wrong when $a = g^{3t} (t \in \mathbb{Z}, t \neq 0)$ because under this condition there will be $a = a^{1+d} = a^{1+2d}$. We correct this fault in the lemma above.

Proposition 4 *Let* $u, v \in \mathbb{F}_{2^{2m}}$ *with* $u \neq v$. *Define a new function* $I_{(u,v)}(x)$ *on* $\mathbb{F}_{2^{2m}}(m \geq 1)$ *as follows:*

$$\begin{cases} I_{(u,v)}(u) = I(v), \\ I_{(u,v)}(v) = I(u), \\ I_{(u,v)}(x) = I(x),\ x \neq u, v \text{ and } x \in \mathbb{F}_{2^{2m}}. \end{cases}$$

Then $\forall (u, v) \in (\mathbb{F}_{2^{2m}} \times \mathbb{F}_{2^{2m}})\ (u \neq v)$, *we have*

$$\delta(I_{(u,v)}) \leq 6.$$

Proof By Proposition 2, $\delta(I_{(u,v)}) \leq 8$. Suppose $\delta(I_{(u,v)}) = 8$. From Proposition 2 and Lemma 3, we know that this happens only when $\Delta_{I_{(u,v)}}(a, b) = \{0, a, ag^d, ag^{2d}, u, u + a, v, v+a\}$ for some $a, b \in \mathbb{F}_{2^{2m}}$, $b = a^{-1} (a \neq 0)$, and the eight elements in $\Delta_{I_{(u,v)}}(a, b)$ are all different. It is easy to see that $u(u + a)v(v + a) \neq 0$ (If not, there must be repeated elements in $\Delta_{I_{(u,v)}}(a, b)$), from these we conclude that

$$\begin{cases} I_{(u,v)}(u) + I_{(u,v)}(u + a) = a^{-1} \\ I_{(u,v)}(v) + I_{(u,v)}(v + a) = a^{-1} \end{cases} \Leftrightarrow \begin{cases} I(v) + I(u + a) = a^{-1} \\ I(u) + I(v + a) = a^{-1} \end{cases}$$

$$\Leftrightarrow \begin{cases} v^{-1} + (u + a)^{-1} = a^{-1} \\ u^{-1} + (v + a)^{-1} = a^{-1} \end{cases} \Rightarrow \begin{cases} ua = a^2 + uv \\ va = a^2 + uv \end{cases} \Rightarrow va = ua.$$

This implies $u = v$ because $a \neq 0$, which is a contradiction. So $\delta(I_{(u,v)})$ cannot reach the maximal value given in Proposition 2, thus $\delta(I_{(u,v)}) \leq 6$. $\square$

Proposition 5 *Let* $I_{(u,v)}$ *be the function defined in Proposition 4,* g *a primitive element in* $\mathbb{F}_{2^{2m}}$. *Then* $\forall t \in \mathbb{Z}$, *we have*

$$I_{(0,g^t)}(x) = g^{2^{2m}-1-t} \sum_{k=0}^{2^{2m}-3} (xg^{2^{2m}-1-t})^k, \tag{7}$$

and

$$\begin{cases} \delta(I_{(0,g^t)}) = 6 \text{ when } m = 2r \\ \delta(I_{(0,g^t)}) \leq 4 \text{ when } m = 2r + 1\ (r \geq 1). \end{cases} \tag{8}$$

Proof It is easy to check that

$$\begin{cases} I_{(0,g^t)}(0) = g^{-t} = I(g^t) \\ I_{(0,g^t)}(g^t) = 0 = I(0) \\ I_{(0,g^t)}(x) = x^{-1} = I(x),\ x \neq 0,\ g^t. \end{cases}$$

So (7) follows.

Now we consider (8). Suppose $\delta(I_{(0,g^t)}) = 6$. Then $\exists (a, b) \in \mathbb{F}^*_{2^{2m}} \times \mathbb{F}_{2^{2m}}$ s.t.

$$\delta_I(a, b) = 4, \quad \delta_{I_{(0,g^t)}}(a, b) = 6, \tag{9}$$

or

$$\delta_I(a, b) = 2, \quad \delta_{I_{(0,g^t)}}(a, b) = 6. \tag{10}$$

Assume (9) is true. Then by Lemma 3 and Proposition 2, there must be

$$\Delta_I(a, b) = \{0, a, ag^d, ag^{2d}\},\ b = a^{-1}$$

and

$$\Delta_{I_{(0,g^t)}}(a,b) = \{0, a, ag^d, ag^{2d}, g^t, g^t + a\}. \quad (11)$$

Based on (11) we have:

$$\begin{cases} I_{(0,g^t)}(0) + I_{(0,g^t)}(a) = b \\ I_{(0,g^t)}(g^t) + I_{(0,g^t)}(g^t + a) = b \end{cases} \Rightarrow \begin{cases} I(g^t) + I(a) = b \\ I(0) + I(g^t + a) = b \end{cases} \Rightarrow b = (g^t + a)^{-1},$$

which contradicts to $b = a^{-1}$. So (9) cannot be true.

Next assume that (10) is true. By Lemma 3 and Proposition 2 we can get

$$\Delta_I(a,b) = \{x_1, x_1 + a\},\ b \neq a^{-1}$$

and

$$\Delta_{I_{(0,g^t)}}(a,b) = \{x_1, x_1 + a, 0, a, g^t, g^t + a\}, \quad (12)$$

and elements in $\Delta_{I_{(0,g^t)}}(a,b)$ are pairwise different.

By (12) we have:

$$I_{(0,g^t)}(x_1) + I_{(0,g^t)}(x_1 + a) = b, \quad (13)$$

and

$$\begin{cases} I_{(0,g^t)}(0) + I_{(0,g^t)}(a) = b \\ I_{(0,g^t)}(g^t) + I_{(0,g^t)}(g^t + a) = b. \end{cases} \quad (14)$$

From (13) we can get

$$I(x_1) + I(x_1 + a) = b \Leftrightarrow x_1^{-1} + (x_1 + a)^{-1} = b$$

$$\Rightarrow (\frac{x_1}{a})^2 + (\frac{x_1}{a}) = (ab)^{-1} \Rightarrow \mathrm{Tr}((ab)^{-1}) = 0. \quad (15)$$

From (14) we can get

$$\begin{cases} I(g^t) + I(a) = b \\ I(0) + I(g^t + a) = b \end{cases} \Leftrightarrow \begin{cases} I(g^t) + I(g^t + \mu) = b \\ I(0) + I(\mu) = b, \end{cases} \quad (16)$$

where $\mu = g^t + a$.

From (16) we know the equation $I(x) + I(x + \mu) = b$ has four different solutions $\{0, \mu, g^t, a\}$. By Lemma 3, the four solutions are $\{0, \mu, \mu g^d, \mu g^{2d}\}$ (Note $b = \mu^{-1}$), so there must be

$$\{0, \mu, g^t, a\} = \{0, \mu, \mu g^d, \mu g^{2d}\}, \quad b = \mu^{-1}. \quad (17)$$

There are no repeated elements in both sets, so one of the following relations must be true:

$$a = \mu g^d, \quad (18)$$

$$a = \mu g^{2d}. \quad (19)$$

Suppose (18) is true. By $b = \mu^{-1}$, we get

$$ab = g^d \Rightarrow (ab)^{-1} = g^{-d} = g^{2d}. \quad (20)$$

By (15) and (20), we conclude that $\mathrm{Tr}((ab)^{-1}) = \mathrm{Tr}(g^{2d}) = 0$, which implies that m is even. (Note that if m is odd, then we have $\mathrm{Tr}(g^{2d}) = \mathrm{Tr}_{2^m/2}(\mathrm{Tr}_{2^n/2^m}(g^{2d})) =$

$\mathrm{Tr}_{2^m/2}(g^{2d}+g^d)=1$, by Lemma 2 and $g^d=g^{4d}$)). If we suppose (19) is true, we will get the same result, the proof is similar, we omit it. Up to now, we have proved:

$$\delta(I_{(0,g^t)})=6 \Rightarrow m=2r\ (r\geq 1).$$

This result and Proposition 4 imply

$$m=2r+1\ (r\geq 1) \Rightarrow \delta(I_{(0,g^t)})\leq 4.$$

In order to confirm this proposition, we still need to prove that:

$$m=2r \Rightarrow \delta(I_{(0,g^t)})=6.$$

Suppose $m=2r$, then $\forall\, g^t (t\in\mathbb{Z})$, considering the following equation

$$(\frac{x}{g^t})^2+(\frac{x}{g^t})=1. \tag{21}$$

By Lemma 1, we know that (21) always has a solution. Suppose a is the solution of (21), it is easy to check that $a\neq 0$ and $a+g^t\neq 0$, so we have

$$(\frac{a}{g^t})^2+(\frac{a}{g^t})=1 \Rightarrow \begin{cases} g^{-t}+a^{-1}=(g^t+a)^{-1} \\ (\frac{a}{g^t})^3=1 \Rightarrow a=g^tg^d \text{ or } a=g^tg^{2d}\ . \end{cases} \tag{22}$$

Let

$$b=g^{-t}+a^{-1}=(g^t+a)^{-1}. \tag{23}$$

Assume $a=g^tg^d$. Then $g^t+a=g^t(g^d+1)=g^tg^{2d}$ (Lemma 2), so $b=(g^t+a)^{-1}=g^{-t}g^{-2d}$. Hence $\mathrm{Tr}((ab)^{-1})=\mathrm{Tr}(g^d)=0$ because $m=2r$ (when $a=g^tg^{2d}$, similar result is also true). By Lemma 1, $x^2+x=(ab)^{-1}$ has a solution $x=c$ in $\mathbb{F}_{2^{2m}}$. It is easy to check that $c\neq 0$, so we can find an element $0\neq x_1\in\mathbb{F}_{2^{2m}}$ such that $\frac{x_1}{a}=c$, then we can get

$$x_1^{-1}+(x_1+a)^{-1}=b. \tag{24}$$

Let $\Delta=\{0,g^t+a,a,g^t,x_1,x_1+a\}$. By (22), (23), (24) and $a=g^tg^d$, it is easy to check that there are no repeated elements in Δ. So By (22), (23), (24), we obtain:

$$\begin{cases} x_1^{-1}+(x_1+a)^{-1}=b \\ g^{-t}+a^{-1}=b \\ (g^t+a)^{-1}=b \end{cases} \Leftrightarrow \begin{cases} I(x_1)+I(x_1+a)=b \\ I(g^t)+I(a)=b \\ I(0)+I(g^t+a)=b \end{cases}$$

$$\Leftrightarrow \begin{cases} I_{(0,g^t)}(x_1)+I_{(0,g^t)}(x_1+a)=b \\ I_{(0,g^t)}(0)+I_{(0,g^t)}(a)=b \\ I_{(0,g^t)}(g^t)+I_{(0,g^t)}(g^t+a)=b, \end{cases}$$

which imply that

$$\delta_{I_{(0,g^t)}}(a,b)\geq \#\Delta_{I_{(0,g^t)}}(a,b)=\{0,g^t+a,a,g^t,x_1,x_1+a\}=\#\Delta=6.$$

From Proposition 4, $\delta(I_{(0,g^t)})\leq 6$, so we can conclude that $m=2r\Rightarrow\delta(I_{(0,g^t)})=6$. Now the first part of (8) is confirmed. □

Remark 1 Simple computation shows that when $m=4, \mathcal{N}(I_{(0,g^t)})=112$; when $m=3$, $\mathcal{N}(I_{(0,g^t)})=24$, which is the same as the inverse function.

Until now, we have introduced some special case about the transformation of the inverse function $I(x)$, next we will give a complete solution about the δ problems of all these transformation functions.

Theorem 1 *Let $I_{(u,v)}$ be defined as in Proposition 4, g be a primitive element in $\mathbb{F}_{2^{2m}}$, $d = \frac{1}{3}(2^{2m}-1)$. Then $\forall i, j \in \mathbb{Z}$ with $g^i \neq g^j$, we have:*

$$\delta(I_{(g^i,g^j)}) = 6 \quad iff \quad \mathrm{Tr}(g^{j-i}) = 0 \text{ or } \mathrm{Tr}(g^{i-j}) = 0, \text{and} \tag{25}$$

$$\delta(I_{(g^i,g^j)}) \leq 4 \quad iff \quad \mathrm{Tr}(g^{j-i}) = 1 \text{ and } \mathrm{Tr}(g^{i-j}) = 1. \tag{26}$$

Proof First, let's consider (25). Suppose $\delta(I_{(g^i,g^j)}) = 6$, then $\exists(a, b)$ s.t.

$$\delta_I(a, b) = 4, \quad \delta_{I_{(g^i,g^j)}}(a, b) = 6, \tag{27}$$

or

$$\delta_I(a, b) = 2, \quad \delta_{I_{(g^i,g^j)}}(a, b) = 6. \tag{28}$$

Assume (27) is true. By Lemma 3 and Proposition 2, there must be

$$\Delta_I(a, b) = \{0, a, ag^d, ag^{2d}\}, \ b = a^{-1} \tag{29}$$

and

$$\Delta_{I_{(g^i,g^j)}}(a, b) \subseteq \Delta_I(a, b) \cup \{g^i, g^i + a, g^j, g^j + a, \}.$$

Because $\Delta_{I_{(g^i,g^j)}}(a, b) = 6$, so there must be

$$g^i \in \Delta_{I_{(g^i,g^j)}}(a, b), \tag{30}$$

or

$$g^j \in \Delta_{I_{(g^i,g^j)}}(a, b). \tag{31}$$

Assume (30) is true. In order to guarantee that there are no repeated elements in $\Delta_{I_{(g^i,g^j)}}(a, b)$, there must be $a + g^i \neq g^j$; otherwise, we can get

$$\begin{cases} a + g^i = g^j \\ b = a^{-1} \\ I_{(g^i,g^j)}(g^i) + I_{(g^i,g^j)}(g^i + a) = b \end{cases} \Leftrightarrow \begin{cases} a = g^i + g^j \\ b = a^{-1} \\ I(g^j) + I(g^i) = b \end{cases}$$

$$\Rightarrow I(g^i + a) + I(g^i) = b \Rightarrow g^i \in \Delta_I(a, b).$$

Together with (29) (30) and the hypothesis $a + g^i = g^j$, it is obviously that there are some repeated elements in $\Delta_{I_{(g^i,g^j)}}(a, b)$. This should not happen, so there must be $a + g^i \neq g^j$. Based on this restriction and (29), (30), we can get

$$\begin{cases} b = a^{-1} \\ I_{(g^i,g^j)}(g^i) + I_{(g^i,g^j)}(g^i + a) = b \end{cases} \Leftrightarrow \begin{cases} b = a^{-1} \\ I(g^j) + I(g^i + a) = b \end{cases}$$

$$\Leftrightarrow \begin{cases} a^{-1} = b \\ \frac{1}{g^j} + \frac{1}{g^i+a} = b \end{cases} \Rightarrow (\frac{a}{g^i})^2 + (\frac{a}{g^i}) = g^{j-i} \Rightarrow \mathrm{Tr}(g^{j-i}) = 0.$$

Similarly, if we assume (31) is true, we can get $\mathrm{Tr}(g^{i-j}) = 0$, so we conclude that if (27) is true, we have

$$\mathrm{Tr}(g^{j-i}) = 0 \ or \ Tr(g^{i-j}) = 0. \tag{32}$$

Next we assume (28) is true. By Lemma 3 and Proposition 2, there must be

$$\Delta_I(a,b) = \{x_1, x_1 + a\}, \ b \neq a^{-1}$$

and

$$\Delta_{I_{(g^i,g^j)}}(a,b) = \{x_1, x_1 + a, g^i, g^i + a, g^j, g^j + a\}. \tag{33}$$

There are no repeated elements in (33) under the condition $\delta_{I_{(g^i,g^j)}}(a,b) = 6$, so we have:

$$\begin{cases} I_{(g^i,g^j)}(x_1) + I_{(g^i,g^j)}(x_1 + a) = b \\ I_{(g^i,g^j)}(g^i) + I_{(g^i,g^j)}(g^i + a) = b \\ I_{(g^i,g^j)}(g^j) + I_{(g^i,g^j)}(g^j + a) = b \end{cases}$$

$$\Leftrightarrow \begin{cases} I(x_1) + I(x_1 + a) = b \\ I(g^j) + I(g^i + a) = b \\ I(g^i) + I(g^j + a) = b \end{cases} \Leftrightarrow \begin{cases} I(x_1) + I(x_1 + a) = b \\ I(g^j) + I(g^j + \mu) = b \\ I(g^i) + I(g^i + \mu) = b, \end{cases} \tag{34}$$

where $\mu = a + g^i + g^j \neq 0$.
By (34) and Lemma 3, we conclude that $\delta_I(\mu, b) = 4$ and there must be $0 \in \Delta_I(\mu, b) = \{g^i, g^i + \mu, g^j, g^j + \mu\}$, since $g^i g^j \neq 0$, so we have

$$g^j + \mu = 0 \tag{35}$$

or

$$g^i + \mu = 0. \tag{36}$$

Assume (35) is true. By (35) and (34), we have

$$(\frac{x_1}{g^i})^2 + (\frac{x_1}{g^i}) = g^{j-i} \Rightarrow \mathrm{Tr}(g^{j-i}) = 0.$$

Similarly, when (36) is true, we get $\mathrm{Tr}(g^{i-j}) = 0$. So if (28) is true, then we have

$$\mathrm{Tr}(g^{j-i}) = 0 \ or \ \mathrm{Tr}(g^{i-j}) = 0. \tag{37}$$

From (32) and (37) we can get

$$\delta_{I_{(g^i,g^j)}} = 6 \Rightarrow \mathrm{Tr}(g^{j-i}) = 0 \ or \ \mathrm{Tr}(g^{i-j}) = 0. \tag{38}$$

Up to now we have proved one side of (25), next we prove the other side of it. Assume $\mathrm{Tr}(g^{j-i}) = 0$, then by Lemma 1, $x^2 + x = g^{j-i}$ must have a solution in $\mathbb{F}_{2^n}$, which implies

$$(\frac{y}{g^i})^2 + (\frac{y}{g^i}) = g^{j-i} \tag{39}$$

has a solution in $\mathbb{F}_{2^{2m}}$. Suppose a is a solution of (39), that is

$$(\frac{a}{g^i})^2 + (\frac{a}{g^i}) = g^{j-i}, \tag{40}$$

which implies

$$\frac{1}{g^j} + \frac{1}{g^i + a} = \frac{1}{a} \ (\text{note } a(a + g^i) \neq 0 \text{ and } a \neq g^i + g^j). \tag{41}$$

Let $b = a^{-1}$, then according to Lemma 3, we know that

$$\Delta_I(a,b) = \{0, a, ag^d, ag^{2d}\}, \text{ where } ag^d + a = ag^{2d}. \tag{42}$$

Define a set

$$\Delta = \{0, a, ag^d, ag^d + a, g^i, g^i + a, g^j, g^j + a\} \text{ where } ag^d + a = ag^{2d}. \tag{43}$$

If there are no repeated elements in Δ, then based on (41) and (42), we can get

$$\delta_{I_{(g^i,g^j)}}(a,b) = \#\Delta_{I_{(g^i,g^j)}}(a,b) = \{0, a, ag^d, ag^{2d}, g^i, g^i + a\} = 6, \tag{44}$$

which is what we want.

Note that there are no duplicate elements in $\Delta_I(a,b)$ (See 42). Define a new set

$$\Gamma = \{g^i, g^i + a, g^j, g^j + a\}.$$

We also assert that elements in Γ are different. For a proof, note that $g^i \neq g^j$ is the premise, we also have $g^i + a \neq g^j$ from (41), so the conclusion follows. We have known that there no repeated elements in $\Delta_I(a,b)$ and Γ, if we can prove

$$\Delta_I(a,b) \cap \Gamma = \emptyset, \tag{45}$$

then we can deduce that elements in Δ are pairwise different. Observe the elements of $\Delta_I(a,b)$ and Δ, in order to confirm this conclusion, we only need to prove that

$$g^i \notin \Delta_I(a,b) \tag{46}$$

and

$$g^j \notin \Delta_I(a,b). \tag{47}$$

Let's prove (46). Assume $g^i \in \Delta_I(a,b)$, $g^i \neq 0$ is obvious, $g^i \neq a$ can be deduced from (40), so if $g^i \in \Delta_I(a,b)$, then there must be

$$g^i = ag^d \tag{48}$$

or

$$g^i = ag^{2d}. \tag{49}$$

Assume (48) is true. Then according to (48) and (41) we can get

$$\frac{1}{g^j} + \frac{1}{ag^d + a} = \frac{1}{a}. \tag{50}$$

Based on (42) we can get

$$\frac{1}{ag^d} + \frac{1}{ag^d + a} = \frac{1}{a}. \tag{51}$$

From (50) and (51) we can conclude that $g^j = ag^d = g^i$, which contradicts the hypothesis that $g^j \neq g^i$. If (49) is true, we will get the same contradiction, so $g^i \notin \Delta_I(a,b)$, (46) is confirmed. With a similar proof, we can also get $g^j \notin \Delta_I(a,b)$, we omit the proof. So (47) is confirmed. From (46) and (47) we deduce that (45) is established, so we obtain that there are no duplicate elements in Δ, based on this constraint and (41) (42) we obtain

$$\begin{cases} I(0)+I(a)=b \\ I(ag^d)+I(ag^d+a)=b \\ I(g^j)+I(g^i+a)=b \end{cases} \Leftrightarrow \begin{cases} I_{(g^i,g^j)}(0)+I_{(g^i,g^j)}(a)=b \\ I_{(g^i,g^j)}(ag^d)+I_{(g^i,g^j)}(ag^d+a)=b \\ I_{(g^i,g^j)}(g^i)+I_{(g^i,g^j)}(g^i+a)=b, \end{cases}$$

which imply (44). Now we can affirm that $\delta_{I_{(g^i,g^j)}}(a,b)=6$. Similarly, if we assume $\mathrm{Tr}(g^{i-j})=0$, we will get the same result. Together with Proposition 4, we have proved that

$$\mathrm{Tr}(g^{j-i})=0 \text{ } or \text{ } \mathrm{Tr}(g^{i-j})=0 \Rightarrow \delta(I_{(g^i,g^j)})=6 \tag{52}$$

Based on (38) and (52), (25) is established.

By Proposition 4, the following assertion is also proved

$$\delta(I_{(g^i,g^j)}) \leq 4 \Leftrightarrow \mathrm{Tr}(g^{j-i})=1 \text{ } and \text{ } \mathrm{Tr}(g^{i-j})=1. \tag{53}$$

□

Let L_1, L_2 be two affine transformations on $\mathbb{F}_{2^n}$. For a function F on $\mathbb{F}_{2^n}$, it is easy to check that $(L_2 \circ F \circ L_1)_{(u,v)} = L_2 \circ F_{(L_1(u),L_1(v))} \circ L_1$, where $u, v \in \mathbb{F}_{2^n}$. Thus the following Corollary follows from Theorem 1:

Corollary 1 *Let L_1, L_2 be two affine transformations on $\mathbb{F}_{2^{2m}}$, and $u, v \in \mathbb{F}_{2^{2m}}$ such that $L_1(u) \neq 0$, and $L_1(v) \neq 0$. Then $(L_2 \circ I \circ L_1)_{(u,v)}$ is differential 4 uniform if and only if $\mathrm{Tr}(L_1(u)L_1(v)^{-1}) = \mathrm{Tr}(L_1(u)^{-1}L_1(v)) = 1$.*

Remark 2 When $m = 4$, all the 32385 different functions support this theorem. There are 9180 functions with differential 4-uniformity property, and the 32385 functions have the same nonlinearity 110, so all the new constructed functions are not CCZ-equivalent to the original inverse function $I(x)$, which has the nonlinearity 112. It can be seen that we really construct some new functions with this method, but we should also note that there are many equivalence relations in the new functions. We also get polynomial form of all the 32385 functions, according to our observation, each polynomial has more than 230 nonzero coefficients, all these polynomials have very complex form. For example, we use the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ to construct the finite field $\mathbb{F}_{2^8}$, g is a root of $x^8 + x^4 + x^3 + x^2 + 1 = 0$, choosing the function $I_{(g^1,g^{12})}$, it is easy to check that $\mathcal{N}(I_{(g^1,g^{12})}) = 110, \delta(I_{(g^1,g^{12})}) = 4$, $A = 477$ (The definition of A can be found in Problem 2). As for $I(x)$, it is well known that $\mathcal{N}(I) = 112, \delta(I) = 4$, the corresponding parameter $A = 255$. (a polynomial form of this function is given in the Appendix).

5 Conclusions

We proposed a method and proved some properties of it in this paper. With this method we partly solved an open problem proposed in [1] and constructed some new differential 4-uniform functions with highly nonlinearity in the even degree fields, which might be useful in the design of cryptographic algorithms.

References

1. T. P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$, IEEE Trans. Inform. Theory 52, no. 9, 4160-4170 (2006).
2. Blondeau, C. Canteaut, A. and P. Charpin. Differential properties of power functions, Int. J. Information and Coding Theory Vol. 1, No. 2, pp.149-170 (2010).
3. C. Brackena, G. Leanderb. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields and Their Applications Volume 16, Issue 4, Pages 231-242, July (2010).
4. K. Browning, J. F. Dillon, R. E. Kibler and M. McQuistan. APN polynomials and related codes. Special volume of Journal of Combinatorics, Information and System Sciences, honoring the 75-th birthday of Prof. D.K.Ray-Chaudhuri, vol. 34, Issue 1-4, pp. 135-159 (2009).
5. L. Budaghyan, C. Carlet and G. Leander. Constructing new APN functions from known ones. Finite Fields and Their Applications Volume 15, Issue 2, Pages 150-159, April (2009).
6. L. Budaghyan, C. Carlet, G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theory 54, 4218-4229 (2008).
7. C. Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Designs, Codes and Cryptography, Online First, 5 January (2011).
8. C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes(185 pages), Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.). In press.
9. C. Carlet. Vectorial Boolean Functions for Cryptography (95 pages). Idem.
10. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography, Vol. 15, No. 2, pp.125-156 (1998).
11. F. Chabaud, S. Vaudenay. Links between differential and linear cryptanalysis. In: Santis A.D. (ed.) Advances in Cryptology-EUROCRYPT 94, vol. 950 of Lecture Notes in Computer Science, pp. 356-365. Springer, New York (1995).
12. J. F. Dillon. APN polynomials: an update, Fq9, The 9th International Conference on Finite Fields and Applications, Dublin, Ireland, July (2009).
13. Y. Edel, A. Pott. A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. 3, 59-81 (2009).
14. H. Dobbertin. One-to-one highly nonlinear power functions on $GF(2^n)$, Applicable Algebra in Engineering, Communication and Computing, Vol. 9, No. 2, pp.139-152 (1998).
15. J.E. Fuller. Analysis of affine equivalent Boolean functions for cryptography. PhD thesis, Queensland University of Technology (2003).
16. R. Lidl, H. Niederreiter, Finite fields. Cambridge, U.K.: Cambridge Univ. Press (1983).
17. K. Nyberg. Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science 765, pp. 55-64 (1994).

Appendix

$$I_{(g^1,g^{12})}(x) = g^{211}x^{1} + g^{189}x^{2} + g^{212}x^{3} + g^{145}x^{4} + g^{236}x^{5} + g^{191}x^{6} + g^{122}x^{7} + g^{57}x^{8} + g^{138}x^{9} + g^{239}x^{10} + g^{144}x^{11} + g^{149}x^{12} + g^{227}x^{13} + g^{11}x^{14} + g^{25}x^{15} + g^{136}x^{16} + g^{233}x^{17} + g^{43}x^{18} + g^{96}x^{19} + g^{245}x^{20} + g^{211}x^{21} + g^{55}x^{22} + g^{5}x^{23} + g^{65}x^{24} + g^{230}x^{25} + g^{221}x^{26} + g^{184}x^{27} + g^{44}x^{28} + g^{210}x^{29} + g^{72}x^{30} + g^{103}x^{31} + g^{39}x^{32} + g^{253}x^{33} + g^{233}x^{34} + g^{137}x^{35} + g^{108}x^{36} + g^{15}x^{37} + g^{214}x^{38} + g^{99}x^{39} + g^{2}x^{40} + g^{19}x^{41} + g^{189}x^{42} + g^{114}x^{43} + g^{132}x^{44} + g^{221}x^{45} + g^{32}x^{46} + g^{36}x^{47} + g^{152}x^{48} + g^{81}x^{49} + g^{227}x^{50} + g^{114}x^{51} + g^{209}x^{52} + g^{88}x^{53} + g^{135}x^{54} + g^{4}x^{55} + g^{110}x^{56} + g^{181}x^{57} + g^{187}x^{58} + g^{133}x^{59} + g^{166}x^{60} + g^{119}x^{61} + g^{228}x^{62} + g^{110}x^{63} + g^{100}x^{64} + g^{170}x^{65} + g^{18}x^{66} + g^{104}x^{67} + g^{233}x^{68} + g^{100}x^{69} + g^{41}x^{70} + g^{36}x^{71} + g^{238}x^{72} + g^{51}x^{73} + g^{52}x^{74} + g^{230}x^{75} + g^{195}x^{76} + g^{133}x^{77} + g^{220}x^{78} + g^{77}x^{79} + g^{26}x^{80} + g^{136}x^{81} + g^{60}x^{82} + g^{208}x^{83} + g^{145}x^{84} + g^{63}x^{85} + g^{250}x^{86} + g^{201}x^{87} + g^{31}x^{88} + g^{46}x^{89} + g^{209}x^{90} + g^{234}x^{91} + g^{86}x^{92} + g^{105}x^{93} + g^{94}x^{94} + g^{114}x^{95} + g^{71}x^{96} + g^{190}x^{97} + g^{184}x^{98} + g^{195}x^{99} + g^{221}x^{100} + g^{250}x^{101} + g^{250}x^{102} + g^{93}x^{103} + g^{185}x^{104} + g^{137}x^{105} + g^{198}x^{106} + g^{10}x^{107} + g^{37}x^{108} + g^{237}x^{109} + g^{30}x^{110} + g^{75}x^{111} + g^{242}x^{112} + g^{155}x^{113} + g^{129}x^{114} + g^{139}x^{115} + g^{141}x^{116} + g^{231}x^{117} + g^{33}x^{118} + g^{216}x^{119} + g^{99}x^{120} + g^{187}x^{121} + g^{5}x^{122} + g^{244}x^{123} + g^{223}x^{124} + g^{12}x^{125} + g^{242}x^{126} + g^{101}x^{127} + g^{222}x^{128} + g^{95}x^{129} + g^{107}x^{130} + g^{50}x^{131} + g^{58}x^{132} + g^{61}x^{133} + g^{230}x^{134} + g^{129}x^{135} + g^{233}x^{136} + g^{37}x^{137} + g^{222}x^{138} + g^{119}x^{139} + g^{104}x^{140} + g^{81}x^{141} + g^{94}x^{142} + g^{168}x^{143} + g^{243}x^{144} + g^{185}x^{145} + g^{124}x^{146} + g^{166}x^{147} + g^{126}x^{148} + g^{46}x^{149} + g^{227}x^{150} + g^{7}x^{151} + g^{157}x^{152} + g^{46}x^{153} + g^{33}x^{154} + g^{246}x^{155} + g^{207}x^{156} + g^{183}x^{157} + g^{176}x^{158} + g^{44}x^{159} + g^{74}x^{160} + g^{41}x^{161} + g^{39}x^{162} + g^{7}x^{163} + g^{142}x^{164} + g^{104}x^{165} + g^{183}x^{166} + g^{155}x^{167} + g^{57}x^{168} + g^{93}x^{169} + g^{148}x^{170} + g^{217}x^{171} + g^{12}x^{172} + g^{106}x^{173} + g^{169}x^{174} + g^{46}x^{175} + g^{84}x^{176} + g^{214}x^{177} + g^{114}x^{178} + g^{163}x^{179} + g^{185}x^{180} + g^{249}x^{181} + g^{235}x^{182} + g^{154}x^{183} + g^{194}x^{184} + g^{186}x^{185} + g^{232}x^{186} + g^{97}x^{187} + g^{210}x^{188} + g^{111}x^{189} + g^{250}x^{190} + g^{167}x^{191} + g^{164}x^{192} + g^{14}x^{193} + g^{147}x^{194} + g^{181}x^{195} + g^{135}x^{196} + g^{176}x^{197} + g^{157}x^{198} + g^{73}x^{199} + g^{209}x^{200} + g^{72}x^{201} + g^{12}x^{202} + g^{120}x^{203} + g^{12}x^{204} + g^{112}x^{205} + g^{208}x^{206} + g^{11}x^{207} + g^{137}x^{208} + g^{120}x^{209} + g^{41}x^{210} + g^{194}x^{211} + g^{163}x^{212} + g^{225}x^{213} + g^{42}x^{214} + g^{12}x^{215} + g^{96}x^{216} + g^{198}x^{217} + g^{241}x^{218} + g^{66}x^{219} + g^{82}x^{220} + g^{165}x^{221} + g^{172}x^{222} + g^{200}x^{223} + g^{251}x^{224} + g^{207}x^{225} + g^{77}x^{226} + g^{153}x^{227} + g^{25}x^{228} + g^{49}x^{229} + g^{45}x^{230} + g^{122}x^{231} + g^{49}x^{232} + g^{86}x^{233} + g^{229}x^{234} + g^{250}x^{235} + g^{88}x^{236} + g^{22}x^{237} + g^{199}x^{238} + g^{89}x^{239} + g^{220}x^{240} + g^{193}x^{241} + g^{141}x^{242} + g^{50}x^{243} + g^{32}x^{244} + g^{114}x^{245} + g^{255}x^{246} + g^{161}x^{247} + g^{213}x^{248} + g^{14}x^{249} + g^{46}x^{250} + g^{197}x^{251} + g^{251}x^{252} + g^{215}x^{253} + g^{14}x^{254}$$