数理解析研究所講究録
第1593巻 2008年 206-212

On an equation over finite fields of characteristic 2 and differentially 4-uniform functions

近畿大学　中川 暢夫 (Nobuo Nakagawa)

1 Introduction

I try to get conditions related to α and β that the following equation over $GF(2^{2e})$ have just two solutions $x = 0$ and $x = 1$ in $GF(2^{2e})$.

$$x^{2^{e+1}} + \alpha x^{2^e} + \beta x^2 + (\alpha + \beta + 1)x = 0 \tag{1}$$

Remark: $x = 0$ and $x = 1$ are solutions of the equation (1)

For example,if we take $e = 3$,

$$x^{16} + \alpha x^8 + \beta x^2 + (\alpha + \beta + 1)x = 0.$$

if we take $e = 4$,

$$x^{32} + \alpha x^{16} + \beta x^2 + (\alpha + \beta + 1)x = 0.$$

It is my motivation to reseach the equation (1) above that we would like to construct APN functions or differentially 4-uniform functions coming from cubic functions of Albert commutative semifields of characteristic 2.

The definitions of APN functions and differentially 4-uniform functions are given as the following.

(The definition of APN functions)
A function $f(x)$ over $GF(2^n)$ is called a **APN**(almost perfect nonlinear) function if

$$f_a(x) := f(x + a) + f(x)$$

is a **two to one** mapping from $GF(2^n)$ to $\mathrm{Im}(f_a)$ for any $a \neq 0$, in other wards the equation

$$f(x + a) + f(x) + f(a) = 0$$

has at most two solutions for any nonzero element a of $GF(2^n)$ if $f(x)$ is quadratic.

Thus APN functions are the characteristic 2 version of planar functions over $GF(p^n)$ for an odd prime p. There exist many APN functions, for example Gold functions,Kasami functions and Dobbertin functions (see [1],[4],[5], [6] and [8]). Until two years ago, known functions as APN functions on $GF(2^n)$, all of them were power functions. However

recently (these two years) several quadratic APN functions which are not power functions and infinite series of quadratic APN functions which are not power functions have been constructed ([1],[2],[7]). It is known that a part of them are CCZ-inequivqlent to any function of known power functions([1]).

(The definition of differentially 4-uniform functions)
A function $f(x)$ over $GF(2^n)$ is called a
differentially 4-uniform function if

$$f_a(x) := f(x+a) + f(x)$$

satisfies $|f_a^{-1}(c)| \leq 4$ for $\forall c \in GF(2^n)$ and any $a \neq 0$, in other wards the equation

$$f(x+a) + f(x) + f(a) = c$$

has at most four solutions for any nonzero element a of $GF(2^n)$ and any element $c \in GF(2^n)$.

APN functions and differentially 4-uniform functions do important roles in recent applications to cryptgraphy.

Albert commutative pre-semifields of characterristic 2 are the following. Let E be the additve group $GF(2^n)$ and the multiplication '$\circ$' is defined in E as

$$x \circ y := xy + \alpha(xy)^\sigma$$

where $\sigma \in \mathrm{Gal}(GF(2^n)/GF(2))$ and $\alpha \notin \{x^{\sigma-1} \mid x \in GF(2^n)\}$. Then the cubic mapping

$$f(x) = (x \circ x) \circ x$$

becomes to

$$f(x) = x^3 + \alpha x^{2\sigma+1} + \alpha x^{3\sigma} + \alpha^{\sigma+1} x^{2\sigma^2+\sigma}.$$

Now we put $n = 2e, t = 2^e$ and $x^\sigma = x^t$, namely σ is the involution of the Galois automorphism group of the extention $GF(2^{2e})/GF(2)$.

Theorem 1. *(N.Nakagawa and S.Yoshiara,[9])*
$f(x) = x^3 + \alpha x^{2t+1} + \alpha x^{3t} + \alpha^{t+1} x^{t+2}$ *is a differentially 4-unifrom function on* $GF(2^{2e})$ *for a primitive element* α.

We will a little modify the above functions as the following.

$$g(x) = x^3 + x^{t+2} + \alpha x^{2t+1} + \alpha^s x^{3t}.$$

It seems that the functions of this form are mountains of treasure of APN functions, by computer calculations of Lilya Budaghyan and Claude Carlet for $3 \leq e \leq 8$.
Take any $a \in GF(2^{2e})(a \neq 0)$. Then

$$g(x+a)+g(x)+g(x) = (ax^2+a^2x)+(a^2x^t+a^tx^2)+\alpha(ax^{2t}+a^{2t}x)+\alpha^s(a^tx^{2t}+a^{2t}x^t).$$

Put $y := x/a$, then $g(x+a)+g(x)+g(x) = 0$ iff $a^3(y^2+y)+a^{t+2}(y^t+y^2)+\alpha a^{2t+1}(y^{2t}+y)+\alpha^s a^{2t}(y^{2t}+y^t) = 0$. Now multiple a^{-3} both of the equation above and put $b := a^{t-1}$ and change y to x again. Then we obtain

$$(x^2+x)+b(x^t+x^2)+\alpha b^2(x^{2t}+x)+\alpha^s b^3(x^{2t}+x^t) = 0.$$

Thus

$$x^{2t}+[(b+\alpha^s b^3)/(\alpha b^2+\alpha^s b^3)]x^t+[(1+b)/(\alpha b^2+\alpha^s b^3)]x^2+[(1+\alpha b^2)/(\alpha b^2+\alpha^s b^3)]x = 0$$

if $\alpha b^2+\alpha^s b^3) \neq 0$.

Namely $g(x)$ is a APN on $GF(2^{2e})$ if the equation above has just two solutions $x = 0$ and $x = 1$ in $GF(2^{2e})$ for any b such that $b^{t+1} = 1$.

2 A solution of the equation (1)

We consider the equation (1) on $GF(2^{2e})$.

$$x^{2t}+\alpha x^t+\beta x^2+\gamma x = 0 \tag{1}$$

where $\gamma = \alpha+\beta+1$ and $t = 2^e$. The following theorem holds.

Theorem 2. *If one of the following conditions is satisfied then the equation* (1) *has exactly two solusions* $x = 0$ *and* $x = 1$ *in* $GF(2^{2e})$.
(1a): $\alpha = 1$ *and* $\beta^{t+1} \neq 1$
(2a): $\alpha(1+\beta)^{t-1} = \alpha^t+\beta^t+1$ *and* $\beta^{t+1} \neq 1$
(3a): $\beta^{t+1} = 1$, $\beta \neq 1$ *and* $\beta(\alpha+1)^{t-1} \neq 1$
(4a): $Q+Q^2+Q^4+\cdots+Q^{t/2} \neq (Q^t+\beta Q)/(\alpha+1)$
where $Q = ((\gamma^t+\beta^t\alpha)(\alpha^{t+1}+\gamma^{t+1}))/(1+\beta^{2t+2})$.

Proof
We have the following equation taking t-power to (1).

$$x^2+\alpha^t x+\beta^t x^{2t}+\gamma^t x^t = 0 \tag{2}$$

By taking β^t multiple of (1),

$$\beta^t x^{2t} + \beta^t \alpha x^t + \beta^{t+1} x^2 + \beta^t \gamma x = 0 \tag{3}$$

Add (2) to (3) We obtain

$$(\gamma^t + \beta^t \alpha) x^t + (1 + \beta^{t+1}) x^2 + (\alpha^t + \beta^t \gamma) x = 0 \tag{4}$$

First of all, we consider the case (i) $\gamma^t + \beta^t \alpha = 0$. Then we have $(1+\alpha)\beta^t = (1+\alpha)^t$. If $\alpha = 1$ and $\beta^{t+1} \neq 1$ then the equation (4) become quadratic and since solusions of (1) are also solusion of (4), the equation (1) has exactly two solusions $x = 0, 1$.

If $\alpha \neq 1$, then $\beta = (1+\alpha)^{(t-1)/t}$. Therefore $\beta^{t+1} = 1$. Thus (4) become the trivial equation. Multiple β^t to (1) We have $\beta^t x^{2t} + \alpha\beta^t x^t + \beta^{t+1} x^2 + (\beta^t \alpha + \beta^{t+1} + \beta^t) x = 0$ namely

$$(\alpha+1)^{t-1} x^{2t} + \alpha(\alpha+1)^{t-1} x^t + x^2 + \alpha^t x = 0.$$

Take $\theta \in GF(2^{2e})$ such that $\theta^t = \alpha$. Then if we substitute $x = \theta$ it satisfies (1) because $\theta^{2t} + \alpha\theta^t = \alpha^2 + \alpha^2 = 0$ and $\theta^2 + \alpha^t \theta = \theta^2 + \theta^2 = 0$. Thus if $(1+\alpha)\beta^t = (1+\alpha)^t$ and $\alpha \neq 1$ the equation (1) has at least 4 solusions.

(ii):The case of $(1+\alpha)\beta^t \neq (1+\alpha)^t$ and $\beta^{t+1} = 1$. Then $Sx^t + Sx = 0$ where $S = \gamma^t + \beta^t \alpha = (1+\alpha)\beta^t + (1+\alpha)^t$. Therefore $x^t = x$ because $S \neq 0$. We have $(1+\beta)(x^2 + x) = 0$ by substituting this to (1). Hence if $1 + \beta \neq 0$, the equation (1) has exactly two solusions $x = 0, 1$.

If $\beta = 1$, then we have $(x^t + x)(x^t + x + \alpha) = 0$ by (1) Hence any element of $GF(2^e)$ are solusions of (1)

(iii):The case of $\alpha^t + \beta^t \gamma = 0$ and $\beta^{t+1} + 1 \neq 0$. This case corresponds to $(2a)$ of the theorem and is contained in $(4a)$ of the theoem.

(iv): The case $(1+\alpha)\beta^t \neq (1+\alpha)^t$ and $\beta^{t+1} \neq 1$.

In this case from (4),

$$x^t = Ax^2 + Bx \tag{5}$$

where $A = (\beta^{t+1} + 1)/(\gamma^t + \beta^t \alpha)$ and $B = (\alpha^t + \beta^t \gamma)/(\gamma^t + \beta^t \alpha)$.
By taking 2-power to this equation we have

$$x^{2t} = A^2 x^4 + B^2 x^2 \tag{6}$$

Substitute (5) and (6) to (1). Then we obtain

$$A^2 x^4 + (B^2 + \alpha A + \beta) x^2 + (\alpha B + \gamma) x = 0 \tag{7}$$

Because $A \neq 0$, it follows that

$$x^4 + Px^2 + Qx = 0 \tag{8}$$

where $P = (B^2 + \alpha A + \beta)/A^2$ and

$$Q = (\alpha B + \gamma)/A^2 = (\alpha(\alpha^t + \beta^t\gamma)(\gamma^t + \beta^t\alpha) + \gamma(\gamma^{2t} + \beta^{2t}\alpha^2))/(\beta^{2t+2} + 1)$$
$$= ((\gamma^t + \beta^t\alpha)(\alpha^{t+1} + \gamma^{t+1}))/(\beta^{2t+2} + 1)$$

Here $1 + P + Q = 0$ holds and

$$P = (\alpha^{2t} + \beta^{2t}\gamma^2)/(\beta^{2t+2} + 1) + \{\alpha(\gamma^t + \beta^t\alpha)\}/(\beta^{t+1} + 1) + \{\beta(\gamma^{2t} + \beta^{2t}\alpha^2)\}/(\beta^{2t+2} + 1).$$

We claim that $\mathrm{Tr}(P) = 0$, therefore $\mathrm{Tr}(Q) = 0$ because $Q = P + 1$, and $\mathrm{Tr}(1) = 0$. Note that $\gamma = \alpha + \beta + 1$.

Because $\mathrm{Tr}(a^2) = \mathrm{Tr}(a)$, the trace value of the sum of the first part and the second part of P is

$$\mathrm{Tr}([(\alpha^t + \beta^t\gamma) + \{\alpha(\gamma^t + \beta^t\alpha)\}]/(\beta^{t+1} + 1))$$
$$= \mathrm{Tr}((\alpha^t + \alpha + \beta^{t+1} + \alpha^{t+1} + (\beta^t + \alpha^2\beta^t))/(\beta^{t+1} + 1)).$$

Now $(\alpha^t + \alpha + \beta^{t+1} + \alpha^{t+1}) \in \mathrm{Fix}(\tau)$ and $(\beta^{t+1} + 1) \in \mathrm{Fix}(\tau)$ where τ is a Galois automorphism of $GF(2^{2e})$ such that $x^\tau := x^t$.

Moreover $\mathrm{Tr}(b) = 0$ for $b \in \mathrm{Fix}(\tau)$
since $\mathrm{Tr}(b) = (b + b^2 + b^4 + \cdots + b^{t/2}) + (b + b^2 + b^4 + \cdots + b^{t/2}) = 0$. Therefore

$$\mathrm{Tr}(P) = \mathrm{Tr}((\beta^t + \alpha^2\beta^t)/(\beta^{t+1} + 1)) + \mathrm{Tr}(\{\beta(\gamma^{2t} + \beta^{2t}\alpha^2)\}/(\beta^{2t+2} + 1))$$
$$= \mathrm{Tr}(\{(\beta^t + \alpha^2\beta^t)(\beta^{t+1} + 1) + \beta(\gamma^{2t} + \beta^{2t}\alpha^2)\}/(\beta^{2t+2} + 1))$$
$$= \mathrm{Tr}(\{(\beta^t + \beta) + (\beta^t\alpha^2 + \beta\alpha^{2t})\}/(\beta^{2t+2} + 1)) = 0,$$

since $\{(\beta^t + \beta) + (\beta^t\alpha^2 + \beta\alpha^{2t})\} \in \mathrm{Fix}(\tau)$.

Thus $\mathrm{Tr}(P) = \mathrm{Tr}(Q) = 0$.

Therefore there is an element $a \in GF(2^{2e})$ such that

$$a^2 + a = Q. \tag{9}$$

From (8) we obtain the following equation.

$$(x^2 + x)(x^2 + x + Q) = 0.$$

Suppose that a is a solusion of (1). Then it holds that

$$a^{2t} + \alpha a^t + \beta a^2 + \gamma a = 0 \tag{10}$$

and

$$a^{2t} + a^t = Q^t. \tag{11}$$

Substitute (9) and (11) to (10). Then we have

$$(\alpha+1)a^t+(\alpha+1)a=Q^t+\beta Q.$$

Thus $a^t+a=(Q^t+\beta Q)/(\alpha+1)$. On the other hand it is clear that $Q+Q^2+Q^4+\cdots+Q^{t/2}=a+a^t$. Hence we obtain

$$Q+Q^2+Q^4+\cdots+Q^{t/2}=(Q^t+\beta Q)/(\alpha+1).$$

Therefore if $Q+Q^2+Q^4+\cdots+Q^{t/2}\neq(Q^t+\beta Q)/(\alpha+1)$, then the equation (1) has just two solusion $x=0$ and $x=1$. **Q.E.D**

We note $(Q+Q^2+Q^4+\cdots+Q^{t/2})\in \mathrm{Fix}(\tau)=GF(2^e)$ because $\mathrm{Tr}(Q)=0$. I calculated the equation of this form on $GF(64)=GF(2)(\theta)$ where $\theta^6=\theta+1$. Only in the cases of $\alpha=\theta$ and β runs on $GF(64)$.

In the case of $(4a)$ of the theorem, roughly speaking about a half cases satisfy the condition $Q+Q^2+Q^4+\cdots+Q^{t/2}\neq(Q^t+\beta Q)/(\alpha+1)$.

For example the equation $x^{16}+\theta x^8+\theta^6x^2=0$ has juat two solutions and $x^{16}+\theta x^8+\theta^2x^2+\theta^{26}x=0$ has four solutions in $GF(64)$.

3 Some results using the theorem in section 2

We constructed several APN functions and differentially 4-uniform functions as the applications of Theorem 2.

Theorem 3.1(N.Nakagawa,[3])

$$f(x)=x^3+x^{2t+1}+\alpha x^{t+2}+\alpha^t x^{3t}$$

is a 4-differentially uniform function over $GF(2^{2e})$ where $t=2^e$ and $GF(2^{2e})^\times=<\alpha>$.

Theorem 3.2(L.Budaghyan and C.Carlet,[3])

$$(1):\quad f(x)=x^3+x^{2t+1}+\gamma x^{t+2}$$

is a APN function over $GF(2^{2e})$ where $t=2^e$, $4\mid e$, $25\not\mid(2^{2e}-1)$ and $GF(4)^\times=<\gamma>$.

$$(2):\quad f(x)=x^3+x^{2t+1}+\gamma x^{t+2}$$

is a APN function over $GF(2^{2e})$ where $t=2^e$, $6\mid e$, $81\not\mid(2^{2e}-1)$ and $GF(8)^\times=<\gamma>$.

Theorem 3.3(L.Budaghyan,[3])

$$f(x) = x^3 + x^{2t+1} + \gamma x^{t+2}$$

is a APN function over $GF(2^{2e})$ where $t = 2^e$, $e = 6k$ and $GF(2^{2e})^\times =< \alpha >$, $\gamma = \alpha^{\frac{2^{2e}-1}{9}}$.

APN functions given in Theorem 3.2 and Theorem 3.3 are EA-equivalent to known power functions. In general a function f is EA-equivalent to a function g if $g(x) = (A_1 f A_2)(x) + A_3(x)$ for affine permutations A_1, A_2 and an affine function A_3 (see [1]).

References

[1] L. Budaghyan, C. Carlet and G.Leander, A class of quadratic APN binomials inequivalent to power functions, submitted.

[2] L. Budaghyan, C. Carlet and A. Pott, New Classes of Almost Bent and Almost Perfect Nonlinear Functions, *IEEE Trans. Inform.Theory*, vol. 52, no. 3 (2006) 1141-1152.

[3] L. Budaghyan,C.Carlet and N.Nakagawa, private communications, 2007.

[4] H. Dobbertin, Almost Perfect Nonlinear Functions, The Welch Case, IEEE Trans. Inform. Theory 45(1999), 1272-1275.

[5] H. Dobbertin, Almost Perfect Nonlinear Functions, The Niho Case, Inform. and Comput. 151(1999), 57-72.

[6] H. Dobbertin, Uniformly representable permutation polynomials, T. Helleseth, P. V. Kumar and K. Yang eds. *in the Proceedings of "Sequences and their applications-SETA '01"*, Springer Verlag, London (2002) 1-22.

[7] Y.Edel, G.Kyureghyan and A.Pott, A new APN function which is not equivalent to a power mapping, *IEEE Trans. Inform. Theory*, vol 52 (2006) 744-747.

[8] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, *Inform. and Control*, 18 (1971) 369-394

[9] N.Nakagawa and S.Yoshiara, A construction of differentially 4-uniform functions from commutative semifields of characteristic 2,in the proceeding of WAIFI07, Springer Lecture Notes in Computer Science,4547 (2007) 134-146.