On the Fourier Spectra of the Infinite Families of Quadratic APN Functions

Carl Bracken[1], Zhengbang Zha[2]

[1]Department of Mathematics, National University of Ireland
Maynooth, Co. Kildare

[2]College of Mathematics and Econometrics, Hunan University
Changsha 410082, China

June 13, 2011

Abstract

It is well known that a quadratic function defined on a finite field of odd degree is almost bent (AB) if and only if it is almost perfect nonlinear (APN). For the even degree case there is no apparent relationship between the values in the Fourier spectrum of a function and the APN property. In this article we compute the Fourier spectrum of the quadranomial family of APN functions from [5]. With this result, all known infinite families of APN functions now have their Fourier spectra and hence their nonlinearities computed.

1   Introduction

Highly nonlinear functions on finite fields are interesting from the point of view of cryptography as they provide optimum resistance to linear and differential attacks. A function that has the APN (resp. AB) property, as defined

below, has optimal resistance to a differential (resp. linear) attack. For more on relations between linear and differential cryptanalysis, see [13].

Highly nonlinear functions are also of interest from the point of view of coding theory. The weight distribution of a certain error-correcting code is equivalent to the Fourier spectrum (including multiplicities) of f. The code having three particular weights is equivalent to the AB property, when n is odd. The minimum distance of the dual code being 5 is equivalent to the APN property holding for f.

For the rest of the paper, let $L = GF(2^n)$ and let L^* denote the set of non-zero elements of L. Let $\mathrm{Tr} : L \to GF(2)$ denote the trace map from L to $GF(2)$.

Definition 1 *A function $f : L \to L$ is said to be* **almost perfect nonlinear (APN)** *if for any $a \in L^*, b \in L$, we have*

$$|\{x \in L : f(x + a) - f(x) = b\}| \leq 2.$$

Definition 2 *Given a function $f : L \to L$, the* **Fourier transform** *of f is the function $\widehat{f} : L \times L^* \to \mathbb{Z}$ given by*

$$\widehat{f}(a, b) = \sum_{x \in L} (-1)^{\mathrm{Tr}(ax + bf(x))}.$$

The *Fourier spectrum* of f is the set of integers

$$\Lambda_f = \{\widehat{f}(a, b) : a, b \in L, b \neq 0\}.$$

The nonlinearity of a function f on a field $L = GF(2^n)$ is defined as

$$NL(f) := 2^{n-1} - \frac{1}{2} \max_{x \in \Lambda_f} |x|.$$

The nonlinearity of a function measures its distance to the set of all affine maps on L. We thus call a function *maximally nonlinear* if its nonlinearity is as large as possible. If n is odd, its nonlinearity is upper-bounded by

$2^{n-1} - 2^{\frac{n-1}{2}}$, while for n even a conjectured upper bound is $2^{n-1} - 2^{\frac{n}{2}-1}$. For odd n, we say that a function $f : L \longrightarrow L$ is *almost bent* (AB) when its Fourier spectrum is $\{0, \pm 2^{\frac{n+1}{2}}\}$, in which case it is clear from the upper bound that f is maximally nonlinear. We have the following connection (for odd n) between the AB and APN property: every AB function on L is also APN [13], and, conversely, if f is quadratic and APN, then f is AB [12]. In particular, quadratic APN functions have optimal resistance to both linear and differential attacks. On the other hand, there appears to be no relation between the nonlinearity $NL(f)$ and the APN property of a function f when n is even. The reader is referred to [10] for a comprehensive survey on APN and AB functions.

2 New Families of Quadratic APN functions

Recently, the first non-monomial families of APN functions have been discovered. Below we list the new families of non monomial functions known at the time of writing.

1.
$$f(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}},$$
   where $n = 3k$, $(k,3) = (s,3k) = 1$, $k \geq 3$, $i \equiv sk \mod 3$, $m \equiv -i$ mod 3, $\alpha = t^{2^k-1}$ and t is primitive (see Budaghyan, Carlet, Felke, Leander [8]).

2.
$$f(x) = x^{2^s+1} + \alpha x^{2^{ik}+2^{mk+s}},$$
   where $n = 4k$, $(k,2) = (s,2k) = 1$, $k \geq 3$, $i \equiv sk \mod 4$, $m = 4 - i$, $\alpha = t^{2^k-1}$ and t is primitive (see Budaghyan, Carlet, Leander [7]). This family generalizes an example found for $n = 12$ by Edel, Kyureghyan, Pott [15].

3.
$$f(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{k+s}+2^k} + \beta x^{2^k+1} + \sum_{i=1}^{k-1} \gamma_i x^{2^{k+i}+2^i},$$

where $n = 2k$, α and β are primitive elements of $GF(2^n)$, and $\gamma_i \in GF(2^k)$ for each i, and $(k,s) = 1$, k is odd, s is odd (see Bracken, Byrne, Markin, McGuire [2]).

4.
$$f(x) = x^3 + Tr(x^9),$$

over $GF(2^n)$, any n (see Budaghyan, Carlet, Leander [9]).

5.
$$f(x) = \alpha^{2^k} x^{2^{-k}+2^{k+s}} + \alpha x^{2^s+1} + v x^{2^{-k}+1} + w \alpha^{2^k+1} x^{2^{k+s}+2^s}$$

where $n = 3k$, α is primitive in $GF(2^n)$, $v, w \in GF(2^k)$ and $vw \neq 1$, $(s, 3k) = 1$, $(3, k) = 1$ and 3 divides $k + s$ (see Bracken, Byrne, Markin, McGuire [5]).

In [1] the Fourier spectra of families (1) and (2) are computed. The determination of the Fourier spectra of families (3) and (4) has been given in [3] and [4], respectively. In this paper we calculate the Fourier spectra of family (5). We will show here that the Fourier spectra of this family of functions are 5-valued $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$ for fields of even degree and 3-valued $\{0, \pm 2^{\frac{n+1}{2}}\}$ for fields of odd degree. In this sense they resemble the Gold functions x^{2^d+1}, $(d, n) = 1$, as indeed do all five APN functions listed above. For fields of odd degree, our result provides another proof of the APN property. This does not hold for fields of even degree; as we stated earlier, there appears to be no relation between the Fourier spectrum and the APN property for fields of even degree. Thus, the fact that f has a 5-valued Fourier spectrum for fields of even degree does not follow from the fact that f is a quadratic APN function. Indeed, there is one example known (due to Dillon

[14]) of a quadratic APN function on a field of even degree whose Fourier spectrum is more than 5-valued; if u is primitive in $GF(2^6)$ then

$$g(x) = x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{33} + x^{48}$$

is a quadratic APN function on $GF(2^6)$ whose Fourier transform takes seven distinct values.

3   The Fourier Spectrum of Family (5)

We shall make use of the following lemma, a proof of which can be found in [1].

Lemma 1 *Let s be an integer satisfying $(s, n) = 1$ and let $f(x) = \displaystyle\sum_{i=0}^{d} r_i x^{2^{si}}$ be a polynomial in $L[x]$. Then $f(x)$ has at most 2^d zeroes in L.*

Theorem 2 *Let $f(x) = \alpha^{2^k}x^{2^{-k}+2^{k+s}} + \alpha x^{2^s+1} + vx^{2^{-k}+1} + w\alpha^{2^k+1}x^{2^{k+s}+2^s}$, where $n = 3k$, α is primitive in $GF(2^n)$, $v, w \in GF(2^k)$ and $vw \neq 1$, $(s, 3k) = 1$, $(3, k) = 1$ and 3 divides $k + s$ The Fourier spectrum of $f(x)$ is $\{0, \pm 2^{\frac{n+1}{2}}\}$ when n is odd and $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$ when n is even.*

Proof: The Fourier spectrum of f is given by

$$\widehat{f}(a, b) = \sum_{x \in L}(-1)^{Tr(ax+bf(x))}.$$

Squaring gives

$$\begin{aligned}
\widehat{f}(a,b)^2 &= \sum_{x \in L}\sum_{y \in L}(-1)^{\text{Tr}(ax+bf(x)+ay+bf(y))} \\
&= \sum_{x \in L}\sum_{u \in L}(-1)^{\text{Tr}(ax+bf(x)+a(x+u)+bf(x+u))},
\end{aligned}$$

from the substitution $y = x + u$.

This becomes

$$\widehat{f}(a,b)^2 = \sum_{u}(-1)^{Tr(au+bf(u))}\sum_{x}(-1)^{Tr(xL_b(u))},$$

5

where

$$L_b(u) := \alpha b u^{2^s} + \alpha^{2^{-s}} b^{2^{-s}} u^{2^{-s}} + \alpha^{2^{-k}} b^{2^k} u^{2^{-k+s}} + \alpha^{2^{-s}} b^{2^{-k-s}} u^{2^{k-s}}$$

$$+ v b^{2^k} u^{2^k} + v b u^{2^{-k}} + w^{2^{-s}} b^{2^{-k-s}} \alpha^{2^{-s}+2^{-k-s}} u^{2^{-k}} + w^{2^{-s}} b^{2^{-s}} \alpha^{2^{k-s}+2^{-s}} u^{2^k}.$$

Using the fact that $\sum_x (-1)^{Tr(cx)}$ is 0 when $c \neq 0$ and 2^n otherwise, we obtain

$$\widehat{f}(a,b)^2 = 2^n \sum_{u \in K} (-1)^{Tr(au+bf(u))},$$

where K denotes the kernel of $L_b(u)$. If the size of the kernel is at most 4, then clearly

$$0 \le \sum_{u \in K} (-1)^{Tr(au+bf(u))} \le 4.$$

Since $\widehat{f}(a,b)$ is an integer, this sum can only be 0, 2, or 4 if n is even, and 1 or 3 if n is odd. The set of permissible values of $\widehat{f}(a,b)$ is then $\{0, 2^{\frac{n+1}{2}}, -2^{\frac{n+1}{2}}\}$ when n is odd and $\{0, 2^{n/2}, -2^{n/2}, 2^{\frac{n+2}{2}}, -2^{\frac{n+2}{2}}\}$ when n is even.

$$\widehat{f}(a,b) \in \begin{cases} \{0, \pm 2^{\frac{n+1}{2}}\} & 2 \nmid n \\ \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\} & 2 \mid n. \end{cases}$$

We must now demonstrate that $|K| \le 4$, which is sufficient to complete the proof.

Now suppose that $L_b(u) = 0$. This gives

$$b^{2^{-k}} L_b(u) = b^{2^{-k}-2^{k-s}} \alpha^{2^{-s}} (b^{2^{-s}+2^{k-s}} u^{2^{-s}} + b^{2^{k-s}+2^{-k-s}} u^{2^{k-s}}$$

$$+ w^{2^{-s}} b^{2^{-s}+2^{k-s}} \alpha^{2^{k-s}} u^{2^k} + w^{2^{-s}} b^{2^{k-s}+2^{-k-s}} \alpha^{2^{-k-s}} u^{2^{-k}})$$

$$+ \alpha^{2^{-k}} b^{2^k+2^{-k}} u^{2^{-k+s}} + \alpha b^{2^{-k}+1} u^{2^s} + v b^{2^k+2^{-k}} u^{2^k} + v b^{2^{-k}+1} u^{2^{-k}} = 0. \qquad (1)$$

Next we let $\theta = \alpha^{2^{-s}} b^{2^{-k}-2^{k-s}}$, $t(u) = b^{2^{-s}+2^{k-s}} (u^{2^{-s}} + w^{2^{-s}} \alpha^{2^{k-s}} u^{2^k})$ and $r(u) = b^{2^k+2^{-k}} (v u^{2^k} + \alpha^{2^{-k}} u^{2^{-k+s}})$. Equation (1) now becomes

$$b^{2^{-k}} L_b(u) = r(u) + r(u)^{2^k} + \theta(t(u) + t(u)^{2^k}) = 0 \qquad (2)$$

6

For convenience we will write $r(u)$ and $t(u)$ as r and t. We have,

$$t^{2^{k+s}} = b^{2^k + 2^{-k}}(u^{2^k} + w\alpha^{2^{-k}}u^{2^{-k+s}}).$$

This implies

$$t^{2^{k+s}} + wr = b^{2^k + 2^{-k}}(1 + vw)u^{2^k}. \tag{3}$$

We also get

$$vt^{2^{k+s}} + r = b^{2^k + 2^{-k}}(1 + vw)\alpha^{2^{-k}}u^{2^{-k+s}}. \tag{4}$$

Equation (3) implies

$$u = b^{-1-2^k}(1 + vw)^{-1}(t^{2^s} + wr^{2^{-k}}),$$

while Equation (4) gives

$$u = b^{-2^{-k-s} - 2^{-s}}(1 + vw)^{-2^{-s}}\alpha^{-2^{-s}}(v^{2^{-s}}t^{2^{-k}} + r^{2^{k-s}}).$$

Combining these two expressions for u yields

$$\theta z(t^{2^s} + wr^{2^{-k}}) = v^{2^{-s}}t^{2^{-k}} + r^{2^{k-s}},$$

where $z = (1 + vw)^{2^{-s}-1}(b^{2^{-k}+2^k+1})^{2^{-s}-1}$. Note $z \in GF(2^k)$. We rearrange and multiply by $\theta + \theta^{2^{-k}}$ to obtain

$$(\theta + \theta^{2^{-k}})(wz\theta^{2^k}r + v^{2^{-s}}t) = (\theta + \theta^{2^{-k}})(\theta^{2^k}zt^{2^{k+s}} + r^{2^{-k-s}}). \tag{5}$$

We claim that $\theta + \theta^{2^{-k}}$ is not zero. If $\theta = \theta^{2^{-k}}$ then $\alpha^{2^k-1} = b^{(2^{k+s}-1)(2^k-2^{-k})}$. As $k + s$ is divisible by 3, $2^{k+s} - 1$ is divisible by seven. This implies α is a seventh power contradicting its primitive status and the claim is proven. From Equation (2) we have

$$r + r^{2^k} = \theta(t + t^{2^k})$$

From this equation and using the fact that relative trace mapping from $GF(2^{3k})$ to $GF(2^k)$ (denoted by Tr_k) is zero for any field element of the form $\delta + \delta^{2^k}$, we derive the following

$$Tr_k(\theta(t + t^{2^k})) = Tr_k(\theta^{-1}(r + r^{2^k})) = 0.$$

As $Tr_k(cg) = cTr_k(g)$ for $c \in GF(2^k)$ and $\theta^{2^{-k}+2^k+1} \in GF(2^k)$ we can say

$$Tr_k((\theta + \theta^{2^{-k}})t) = Tr_k(\theta^{2^k}(\theta + \theta^{2^{-k}})r) = 0. \qquad (6)$$

Therefore the left hand side of Equation (5) has relative trace of zero, which implies the right hand side of Equation (5) has relative trace of zero also. That is,

$$Tr_k((\theta + \theta^{2^{-k}})(\theta^{2^k}zt^{2^{k+s}} + r^{2^{-k-s}})) = 0.$$

We write this as

$$z((\theta + \theta^{2^{-k}})\theta^{2^k}t^{2^{k+s}} + (\theta + \theta^{2^{-k}})^{2^k}\theta^{2^{-k}}t^{2^{-k+s}} + (\theta + \theta^{2^{-k}})^{2^{-k}}\theta t^{2^s})$$

$$= (\theta + \theta^{2^{-k}})r^{2^{-k-s}} + (\theta + \theta^{2^{-k}})^{2^k}r^{2^{-s}} + (\theta + \theta^{2^{-k}})^{2^{-k}}r^{2^{k-s}}. \qquad (7)$$

From Equation (6) we obtain

$$t^{2^{-k+s}} = (\theta + \theta^{2^{-k}})^{2^s - 2^{-k+s}}t^{2^s} + (\theta + \theta^{2^{-k}})^{2^{k+s} - 2^{-k+s}}t^{2^{k+s}},$$

$$r^{2^{-k-s}} = \theta^{2^{k-s} - 2^{-s}}(\theta + \theta^{2^{-k}})^{2^{-s} - 2^{-k-s}}r^{2^{-s}} + \theta^{2^{-k-s} - 2^{-s}}(\theta + \theta^{2^{-k}})^{2^{k-s} - 2^{-k-s}}r^{2^{k-s}}.$$

Substituting these expressions for $t^{2^{-k+s}}$ and $r^{2^{-k-s}}$ into Equation (7) we get

$$z(((\theta + \theta^{2^{-k}})\theta^{2^k} + (\theta + \theta^{2^{-k}})^{2^k}\theta^{2^{-k}}(\theta + \theta^{2^{-k}})^{2^{k+s} - 2^{-k+s}})t^{2^{k+s}} +$$

$$((\theta + \theta^{2^{-k}})^{2^{-k}}\theta + (\theta + \theta^{2^{-k}})^{2^k}\theta^{2^{-k}}(\theta + \theta^{2^{-k}})^{2^s - 2^{-k+s}})t^{2^s})$$

$$= ((\theta + \theta^{2^{-k}})^{2^k} + (\theta + \theta^{2^{-k}})\theta^{2^{k-s} - 2^{-s}}(\theta + \theta^{2^{-k}})^{2^{-s} - 2^{-k-s}})r^{2^{-s}} +$$

$$((\theta + \theta^{2^{-k}})^{2^{-k}} + (\theta + \theta^{2^{-k}})\theta^{2^{-k-s} - 2^{-s}}(\theta + \theta^{2^{-k}})^{2^{k-s} - 2^{-k-s}})r^{2^{k-s}}.$$

We multiply across by $(\theta + \theta^{2^{-k}})^{2^{-k-s} + 2^{-k+s}}\theta^{2^{-s}}$ and obtain

$$z(\theta + \theta^{2^{-k}})^{2^{-k-s}}\theta^{2^{-s}}(((\theta + \theta^{2^{-k}})^{2^{-k+s}+1}\theta^{2^k} + (\theta + \theta^{2^{-k}})^{2^{k+s}+2^k}\theta^{2^{-k}})t^{2^{k+s}}$$

$$+((\theta + \theta^{2^{-k}})^{2^{-k+s}+2^{-k}}\theta + (\theta + \theta^{2^{-k}})^{2^s+2^k}\theta^{2^{-k}})t^{2^s}) =$$

$$(\theta + \theta^{2^{-k}})^{2^{-k+s}}(((\theta + \theta^{2^{-k}})^{2^{-k-s}+2^k}\theta^{2^{-s}} + (\theta + \theta^{2^{-k}})^{2^{-s}+1}\theta^{2^{k-s}})r^{2^{-s}}$$

$$+((\theta + \theta^{2^{-k}})^{2^{-k-s}+2^{-k}}\theta^{2^{-s}} + (\theta + \theta^{2^{-k}})^{2^{k-s}+1}\theta^{2^{-k-s}})r^{2^{k-s}}).$$

Letting $P(\theta) = (\theta + \theta^{2^{-k}})^{2^{-k+s}+1}\theta^{2^k} + (\theta + \theta^{2^{-k}})^{2^{k+s}+2^k}\theta^{2^{-k}}$, the above equation becomes

$$z(\theta + \theta^{2^{-k}})^{2^{-k-s}}\theta^{2^{-s}}(P(\theta)t^{2^{k+s}} + P(\theta)^{2^{-k}}t^{2^s})$$

$$= (\theta + \theta^{2^{-k}})^{2^{-k+s}}(P(\theta)^{2^{-k-s}}r^{2^{-s}} + P(\theta)^{2^{k-s}}r^{2^{k-s}}). \qquad (8)$$

We claim that $P(\theta)$ is a non zero element of $GF(2^k)$. Setting $P(\theta)$ equal to zero yields

$$(\theta + \theta^{2^{-k}})^{2^{-k+s}+1}\theta^{2^k} = (\theta + \theta^{2^{-k}})^{2^{k+s}+2^k}\theta^{2^{-k}}.$$

This implies

$$\theta^{2^k - 2^{-k}} = (\theta + \theta^{2^{-k}})^{(2^{k+s}-1)(1-2^{-k})}.$$

Therefore $\theta^{2^k - 2^{-k}}$ is a seventh power. But $\theta^{2^k - 2^{-k}} = (\alpha b^{2^k(2^{k+s}-1)})^{2^k - 2^{-k}}$, which would require α to be a seventh power also, which its not. Hence $P(\theta) \neq 0$.

To see that $P(\theta) \in GF(2^k)$, we multiply the expression out and refactor as follows.

$$P(\theta) = (\theta + \theta^{2^{-k}})^{2^{-k+s}}(\theta + \theta^{2^{-k}})\theta^{2^k} + (\theta + \theta^{2^{-k}})^{2^{k+s}}(\theta + \theta^{2^{-k}})^{2^k}\theta^{2^{-k}}.$$

This implies

$$P(\theta) = (\theta^{2^{-k+s}} + \theta^{2^{k+s}})(\theta^{2^k+1} + \theta^{2^{-k}+2^k}) + (\theta^{2^s} + \theta^{2^{k+s}})(\theta^{2^{-k}+1} + \theta^{2^{-k}+2^k}),$$

which becomes

$$P(\theta) = \theta^{2^s}(\theta^{2^{-k}+1} + \theta^{2^{-k}+2^k}) + \theta^{2^{k+s}}(\theta^{2^k+1} + \theta^{2^{-k}+1}) + \theta^{2^{-k+s}}(\theta^{2^k+2^{-k}} + \theta^{2^k+1}).$$

We can write this as

$$P(\theta) = Tr_k(\theta^{2^s}(\theta^{2^{-k}+1} + \theta^{2^{-k}+2^k})),$$

hence $P(\theta) \in GF(2^k)$ and the claim is proven.

Now Equation (8) becomes

$$z(\theta + \theta^{2^{-k}})^{2^{-k-s}-2^{-k+s}}P(\theta)^{1-2^{-s}}(t + t^{2^k})^{2^s} = \theta^{-2^{-s}}(r + r^{2^k})^{2^{-s}}.$$

Using Equation (2) and raising by 2^s we obtain an equation in $(t + t^{2^k})$,

$$z^{2^s}(\theta + \theta^{2^{-k}})^{2^{-k}-2^{-k+2s}}P(\theta)^{2^s-1}(t + t^{2^k})^{2^{2s}} + (t + t^{2^k}) = 0,$$

which by Lemma 1 can have no more than two solutions for $(t + t^{2^k})$ when n is odd and no more than four solutions for $(t + t^{2^k})$ when n is even. This restriction on $(t + t^{2^k})$ is crucial and will be used to complete the proof, but first we consider the following two expressions which come from Equations (3) and (4) respectively,

$$Bu = t^{2^s} + wr^{2^{-k}},$$

$$\alpha^{2^{-s}}B^{2^{-k-s}}u = v^{2^{-s}}t^{2^{-k}} + r^{2^{k-s}},$$

where $B = (1 + vw)b^{2^k+1}$. From these we obtain

$$Bu + B^{2^k}u^{2^k} = (t + t^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}},$$

$$\alpha^{2^{-s}}B^{2^{-k-s}}u + \alpha^{2^{k-s}}B^{2^{-s}}u^{2^k} = v^{2^{-s}}(t + t^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}}.$$

Next we eliminate the u^{2^k} term in these equations to give the following

$$(\alpha^{2^{k-s}}B^{2^{-s}+1} + \alpha^{2^{-s}}B^{2^{-k-s}+2^k})u = B^{2^k}(v^{2^{-s}}(t + t^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}})$$

$$+ \alpha^{2^{k-s}}B^{2^{-s}}((t + t^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}}). \tag{9}$$

We let $D = \alpha^{2^{k-s}}B^{2^{-s}+1} + \alpha^{2^{-s}}B^{2^{-k-s}+2^k}$ and note that D is not zero as $D = 0$ implies $\alpha^{2^{k-s}-2^{-s}} = B^{2^{-k-s}+2^k-2^{-s}-1} = B^{(2^{k+s}-1)(2^{-s}-2^{-k-s})}$, which again contradicts the fact that α is primitive. Therefore we may write Equation (9) as

$$u = D^{-1}(B^{2^k}(v^{2^{-s}}(t + t^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}})$$

$$+ \alpha^{2^{k-s}}B^{2^{-s}}((t + t^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}})).$$

We now use Equation (2) to substitute the $r + r^{2^k}$ terms for $\theta(t + t^k)$ and we obtain

$$u = D^{-1}(B^{2^k}(v^{2^{-s}}(t + t^{2^k})^{2^{-k}} + (\theta(t + t^k))^{2^{k-s}})$$

$$+ \alpha^{2^{k-s}}B^{2^{-s}}((t + t^{2^k})^{2^s} + w(\theta(t + t^k))^{2^{-k}})).$$

Recall $t + t^{2^k}$ can only take two values when n is odd and four when n is even, hence the above equation shows that u must have at least the same restrictions and the proof is complete.

References

[1] C. Bracken, E. Byrne, N. Markin, G. McGuire, "On the Fourier spectrum of Binomial APN functions", *SIAM journal of Discrete Mathematics*, to appear.

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials", *Finite Fields and Applications*, Vol. 14, Issue 3, July 2008, 703–714.

[3] C. Bracken, E. Byrne, N. Markin, G. McGuire, "Determining the Nonlinearity of a New Family of APN Functions", *Applied Algebra, Algebraic Algorithms and Error Correcting Codes*, Lecture Notes in Computer Science, Vol 4851, Springer-Verlag, 2007, 72–79.

[4] C. Bracken, E. Byrne, N. Markin, G. McGuire, "On the Walsh Spectrum of a New APN Function," *Cryptography and Coding*, Lecture Notes in Computer Science, Vol 4887, Springer-Verlag, 2007, 92–98.

[5] C. Bracken, E. Byrne, N. Markin, G. McGuire, "A few more quadratic APN functions", *Cryptography and Communications*, to appear.

[6] L. Budaghyan, C. Carlet and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions," *IEEE Transactions on Information Theory*, Vol. 54, Issue 9, Sep. 2008, 4218–4229.

[7] L. Budaghyan, C. Carlet, G. Leander, "Another class of quadratic APN binomials over F_{2^n}: the case n divisible by 4," *Proceedings of WCC 07*, Versailles, France, April 2007, 49–58.

[8] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, "An infinite class of quadratic APN functions which are not equivalent to power mappings", *Proceedings of ISIT 2006*, Seattle, USA, July 2006.

[9] L. Budaghyan, C. Carlet, G. Leander, "Constructing new APN functions from known ones", *Finite Fields Appl.*, to appear.

[10] C. Carlet, "Vectorial Boolean functions for Cryptography", to appear as a chapter of the monograph *Boolean methods and models*, Cambridge University Press (Ed. Peter Hammer and Yves Crama), available at http://www-rocq.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf.

[11] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility of cyclic codes, highly nonlinear functions on GF(2m) and crosscorrelation of maximum-length sequences," *SIAM Journal on Discrete Mathematics*, 13 (1), 2000, 105–138.

[12] C. Carlet, P. Charpin, V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems ", *Designs, Codes and Cryptography*, Vol. 15, No. 2, 1998, 125–156.

[13] F. Chabaud, S. Vaudenay. "Links between differential and linear cryptanalysis, *Advances in Cryptology EUROCRYPT94*, Lecture Notes in Computer Science, Vol. 950 Springer-Verlag, 1995.

[14] John Dillon, slides from talk given at "Polynomials over Finite Fields and Applications", held at Banff International Research Station, November 2006.

[15] Y. Edel, G. Kyureghyan, A. Pott, "A new APN function which is not equivalent to a power mapping", *IEEE Transactions on Information Theory*, Vol. 52, Issue 2, Feb. 2006, 744–747.

[16] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in Cryptology EUROCRYPT93*, Lecture Notes in Computer Science, Springer-Verlag, 1994, 55–64.