Quadratic Almost Perfect Nonlinear Functions With Many Terms

Carl Bracken [1]

Eimear Byrne [2]

Nadya Markin [3]

Gary McGuire [2]

School of Mathematical Sciences
University College Dublin
Ireland

Abstract

We introduce a new infinite family of multiterm functions that are APN on $GF(2^{2k})$ for odd k.

Key words: almost perfect nonlinear, bent function, CCZ equivalence, Fourier spectrum

Email addresses: carlbracken@yahoo.com (Carl Bracken), ebyrne@ucd.ie (Eimear Byrne), nadyaomarkin@gmail.com (Nadya Markin), gary.mcguire@ucd.ie (Gary McGuire).

[1] Research supported by Irish Research Council for Science, Engineering and Technology Postdoctoral Fellowship.

[2] Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

[3] Postdoctoral fellow funded by the Claude Shannon Institute.

1 Introduction

Let $L = \mathbb{F}_{2^n}$, the finite field with 2^n elements for some positive integer n. A function $f : L \longrightarrow L$ is said to be *almost perfect nonlinear* (APN) if the number of roots in L of the polynomial

$$f(x+a) + f(x) + b$$

is at most 2, for all $a, b \in L$, $a \neq 0$. If the number of roots in L is at most δ, we say f is differentially δ-uniform. Thus APN is the same as differentially 2-uniform. A differentially 1-uniform function is also called a perfect nonlinear function; these do not exist in characteristic 2.

APN functions were introduced in [8] by Nyberg, who defined them as the mappings with highest resistance to differential cryptanalysis. Since then many papers have been written on APN functions, although not many different families of such functions are known. Indeed, a recent result of Voloch [10] shows that APN functions asymptotically have density 0 in the set of all functions, in a certain sense.

Two functions $f, g : L \longrightarrow L$ are called *extended affine* (EA) equivalent if there exist affine permutations A_1, A_2 and an affine map A such that $g = A_1 \circ f \circ A_2 + A$. The differential uniformity of a function is an invariant of EA equivalence. However, a bijective function is not necessarily EA equivalent to its inverse, even though they have the same differential uniformity.

Until recently, all known APN functions were EA equivalent to one of a short list of monomial functions, namely the Gold, Kasami-Welch, inverse, Welch, Niho and Dobbertin functions. For some time it was conjectured that this list was the complete list of APN functions up to EA equivalence.

A more general notion of equivalence has been suggested in [5], which is referred to as Carlet-Charpin-Zinoviev (CCZ) equivalence. Two functions are called CCZ equivalent if the graph of one can be obtained from the graph of the other by an affine permutation of the product space. Differential uniformity and resistance to linear, differential and algebraic attacks are invariants of CCZ equivalence, and any permutation is CCZ equivalent to its inverse.

EA equivalence is a special case of CCZ equivalence. In [3], Proposition 3, the authors express necessary and sufficient conditions for EA equivalence of functions in terms of CCZ equivalence and use this to construct several examples of APN functions that are CCZ equivalent to the Gold functions but EA inequivalent to any monomial function. This showed that the original conjecture is false. The new question was whether all APN functions are CCZ equivalent to one on the list.

In 2006 a sporadic example of a binomial APN function that is CCZ inequivalent to any power mapping was given in [7]. A family of APN binomials on fields $\mathbb{F}_{2^n}$ where n is divisible by 3 but not 9 was presented in [1]. In [2] these have been shown to be EA inequivalent to any monomial function, and CCZ inequivalent to the Gold or Kasami-Welch functions. Dillon [6] presented a family of hexanomials whose members are differentially 4-uniform. Motivated by this family, we introduce a new class of APN functions on fields of order 2^{2k} where k is odd.

Let k and s be a pair of odd coprime integers. The polynomials we have discovered are

$$bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i x^{2^{i+k}+2^i} \tag{1}$$

where $b, c \in \mathbb{F}_{2^{2k}}$, and $r_i \in \mathbb{F}_{2^k}$ for each i. These polynomials have coefficients in $\mathbb{F}_{2^{2k}}$, and have up to $k+3$ nonzero coefficients, depending on the choice of the r_i, some or all of which could be 0. They are motivated by Dillon's polynomials, and are defined on different fields to the binomials in [1] in general.

Let Tr denote the trace map from L to $\mathbb{F}_2$. The Fourier transform of any real-valued function F defined on L is the function $\widehat{F}$ defined by

$$\widehat{F}(a) = \sum_{x \in L} F(x)(-1)^{\mathrm{Tr}(ax)}$$

for $a \in L$. The Fourier spectrum of F is the set $\{\widehat{F}(a) : a \in L\}$ of values of $\widehat{F}$.

To a Boolean function $f : L \longrightarrow \mathbb{F}_2$ we associate the real-valued function $F = (-1)^f$. When we refer to the Fourier spectrum of f, we mean the Fourier spectrum of the associated function $F = (-1)^f$. For arbitrary f, computing its Fourier spectrum is often difficult.

Bent functions were introduced in [9] by Rothaus in 1976 as Boolean functions having maximal distance to the set of all affine Boolean functions (the first order Reed-Muller code). Equivalently, the bent functions on L are precisely those whose Fourier spectrum is $\{\pm\sqrt{|L|}\}$.

In Section 2 we prove that the trace of (1) is a bent function. In Section 3 we show that if $b, c \notin \mathbb{F}_{2^k}$, and b is not a cube, then a polynomial of the form (1) is APN. In a later article we will discuss the inequivalence of these APN functions to power mappings.

The existence of a bijective APN function on $\mathbb{F}_{2^n}$ for n even is an open question. We remark that the polynomials (1) are not bijective. It is easy to verify that $f(\alpha\beta) = f(\alpha\beta + \beta)$ where $\alpha^{2^k} + \alpha + 1 = 0$ and $\beta = b^{-(2^s+1)}$.

Notation: For the remainder, let n be a positive integer. Let k and s be odd relatively prime integers. Let L and K be the finite fields of orders 2^n and 2^{2k} respectively.

2 Proof of Bent Property

An interesting property of the polynomials

$$f(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i x^{2^{i+k}+2^i}$$

is that $\mathrm{Tr}(f(x))$ is a bent function on K. We include a proof below using standard techniques.

Theorem 1 *Let*

$$f(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{j=0}^{k-1} r_j x^{2^{k+j}+2^j}$$

be a function on K with $c \notin \mathbb{F}_{2^k}$ and $r_j \in \mathbb{F}_{2^k}$ for each j. Then the Boolean function $\mathrm{Tr}(f(x))$ is bent.

Proof: We need to show that the Fourier transform $\widehat{F}(r)$, of $F(x) = \mathrm{Tr}(f(x))$, is limited to the two values $\pm 2^k$.

By definition

$$\widehat{F}(r) = \sum_{x \in K} (-1)^{\mathrm{Tr}(rx+f(x))}.$$

Squaring gives

$$\widehat{F}(r)^2 = \sum_y \sum_x (-1)^{\mathrm{Tr}(rx+f(x)+ry+f(y))}.$$

Replacing y with $x+u$ we have

$$\widehat{F}(r)^2 = \sum_u \sum_x (-1)^{\mathrm{Tr}(ru+f(x)+f(x+u))} = \sum_u (-1)^{\mathrm{Tr}(ru+f(u))} \sum_x (-1)^{\mathrm{Tr}(\Delta_u(x))},$$

where $\Delta_u(x) = f(u) + f(x) + f(x+u)$.

Since $r_j^{2^k} = r_j$ for each j, we may write

$$\Delta_u(x) = c(x^{2^{k+s}}u^{2^s} + x^{2^s}u^{2^{k+s}}) + b(x^{2^s}u + xu^{2^s}) + (b(x^{2^s}u + xu^{2^s}))^{2^k} +$$

$$\sum_{j=0}^{k-1} \left(r_j x^{2^{j+k}} u^{2^j} + (r_j x^{2^{j+k}} u^{2^j})^{2^k} \right)$$

so taking trace gives the simplification

$$\mathrm{Tr}(\Delta_u(x)) = \mathrm{Tr}(c(x^{2^{k+s}}u^{2^s} + x^{2^s}u^{2^{k+s}})).$$

Simplifying gives

$$\widehat{F}(r)^2 = \sum_u (-1)^{\mathrm{Tr}(ru + Au^{2^k+1})} \left(\sum_x (-1)^{\mathrm{Tr}(xL(u))} \right)$$

where $A = c^{2^{-s}} + \sum_{j=0}^{k-1} r_j^{2^{-j}}$, $L(u) = (c + c^{2^k})^{2^{-s}} u^{2^k}$. Since $c \notin \mathbb{F}_{2^k}$, $L(u) \neq 0$ except when $u = 0$. This means that the inner sum is 0 except when $u = 0$. Hence $\widehat{F}(r)^2 = 2^{2k}$ and the proof is complete. □

In [4] it is noted that $\mathrm{Tr}(vf(x))$ will be bent for at least $\frac{2}{3}(2^n - 1)$ values of v for any quadratic APN function on L. The same argument as in the proof of the previous theorem shows that $Tr(vf(x))$ is bent for $v \in \mathbb{F}_{2^k}$.

3 Proof of APN Property

We shall now prove that the polynomials (1) are APN under certain conditions.

Theorem 2 *Let f be the function on K defined by*

$$f(x) = bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i x^{2^{i+k}+2^i}$$

where $b, c \notin \mathbb{F}_{2^k}$, b is not a cube, and $r_i \in \mathbb{F}_{2^k}$ for each i. Then f is APN over K.

Proof: To prove that f is APN we must show that the equation

$$f(x) + f(x+q) = p \tag{2}$$

has at most two solutions for all $p \in K$ and all $q \in K^*$.

Equation 2 gives the expression

$$bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i x^{2^{i+k}+2^i} + b(x+q)^{2^s+1}$$
$$+b^{2^k}(x+q)^{2^{k+s}+2^k} + c(x+q)^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i (x+q)^{2^{i+k}+2^i} = p.$$

Replacing x with xq and rearranging we obtain

$$Ax + Bx^{2^k} + Cx^{2^s} + Dx^{2^{k+s}} + \sum_{j=1}^{k-1} R_j(x^{2^{k+j}} + x^{2^j}) = E \tag{3}$$

where

$$A = r_0 q^{2^k+1} + bq^{2^s+1}, \quad B = r_0 q^{2^k+1} + b^{2^k} q^{2^{k+s}+2^k}, \quad C = bq^{2^s+1} + cq^{2^{k+s}+2^s},$$
$$D = b^{2^k} q^{2^{k+s}+2^k} + cq^{2^{k+s}+2^s}, \quad E = f(q) + p, \quad \text{and } R_j = r_j q^{2^{k+j}+2^j},$$

for each j.

As Equation (3) is affine, for the purposes of counting the number of its solutions we may assume $E = 0$.

Define

$$\Delta(x) := Ax + Bx^{2^k} + Cx^{2^s} + Dx^{2^{k+s}} + \sum_{j=1}^{k-1} R_j(x^{2^{k+j}} + x^{2^j}).$$

Then f is APN on K if and only the equation $\Delta(x) = 0$ has at most two solutions in K. Obviously 0 is a solution of $\Delta(x) = 0$, and 1 is a solution of $\Delta(x) = 0$ because $\Delta(1) = A + B + C + D = 0$. We will now show there are no other solutions in K.

Consider

$$\Delta(x) + (\Delta(x))^{2^k} = (C + D^{2^k})(x^{2^s} + x^{2^{k+s}}) = (c + c^{2^k})q^{2^{k+s}+2^s}(x^{2^s} + x^{2^{k+s}}).$$

As $q \neq 0$ and $c \notin \mathbb{F}_{2^k}$, the above expression with $\Delta(x) = 0$ implies $x^{2^s} + x^{2^{k+s}} = 0$, which means $x \in \mathbb{F}_{2^k}$. We can now write

$$\Delta(x) = (A + B)x + (C + D)x^{2^s} = (A + B)(x + x^{2^s}) = 0.$$

Since $(2k, s) = 1$ it remains to show that $A + B \neq 0$. Suppose that $A + B = 0$. Then

$$bq^{2^s+1} + b^{2^k} q^{2^{k+s}+2^k} = 0,$$

which implies

$$b^{2^k-1} = q^{(2^{k+s}-1)(2^k-1)}.$$

Using the fact that 3 divides $2^t - 1$ if and only if t is even, and recalling that we chose b not to be a cube, we see that the left-hand side of this equation is not a cube. As $k + s$ is even, the right hand side of this expression is a cube. Hence $A + B \neq 0$.

Acknowledgement: We thank John Dillon for sharing the slides from his talk at Banff.

References

[1] 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.

[2] L. Budaghyan, C. Carlet, G. Leander, "A class of quadratic APN binomials inequivalent to power functions, preprint.

[3] L. Budaghyan, C. Carlet, A. Pott, " New constructions of almost bent and almost perfect nonlinear functions", *IEEE Transactions on Information Theory*, Vol. 52, No. 3, pp. 1141-1152, March 2006.

[4] C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes", to appear as a chapter of the monography *Boolean methods and models*, Cambridge University Press (Ed. Peter Hammer and Yves Crama).

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

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

[7] 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, pp. 744-747, Feb. 2006.

[8] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 55-64, 1994.

[9] O. Rothaus, "On bent functions," Journal of Combinatorial Theory Series A, Vol. 20, pp. 181-199, 1976.

[10] J. F. Voloch, Symmetric Cryptography and Algebraic Curves, preprint.