Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 146-151*

Binary quasi-perfect linear codes from APN quadratic functions[1]

Chunlei Li Chunlei.Li@ii.uib.no
Tor Helleseth Tor.Helleseth@ii.uib.no
University of Bergen, NORWAY

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. A mapping f from $\mathbb{F}_{2^m}$ to itself is almost perfect nonlinear (APN) if its directional derivatives in nonzero directions are all 2-to-1. Let $\mathcal{C}_f$ be the binary linear code of length 2^m-1, whose parity check matrix has its j-th column $\begin{bmatrix} \pi^j \\ f(\pi^j) \end{bmatrix}$, where π is a primitive element in $\mathbb{F}_{2^m}$ and $j=0,1,\cdots,2^m-2$. For $m \geq 3$ and any quadratic APN function $f(x)=\sum_{i,j=0}^{m-1} a_{i,j}x^{2^i+2^j}$, $a_{i,j} \in \mathbb{F}_{2^m}$, it is proved that $\mathcal{C}_f$ is a quasi-perfect code. As a consequence this gives many classes of binary linear codes with minimum distance 5 and covering radius 3.

1 Background

Let q be a power of a prime p, $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$. The minimum (Hamming) distance d of a code $\mathcal{C}$ defines its error-correcting properties: $e = \lfloor \frac{d-1}{2} \rfloor$, which is known as the packing radius of the code $\mathcal{C}$. The covering radius ϱ of a code $\mathcal{C}$ is the smallest possible integer such that the spheres of this radius around the codewords cover the whole space $\mathbb{F}_q^n$, i.e.,

$$\varrho = \max_{x \in \mathbb{F}_q^n} \min_{\mathbf{c} \in \mathcal{C}} d(x, \mathbf{c}).$$

In particular, if the code $\mathcal{C}$ is linear, the covering radius can be equivalently defined in terms of its parity-check matrix as follows.

Definition 1. *Let $\mathcal{C}$ be an $[n,k]$ code with parity-check matrix H. The covering radius of $\mathcal{C}$ is the smallest integer ϱ such that every q-ary $(n-k)$-dimensional column vector can be written as a linear combination of at most ϱ columns from H.*

Obviously, the covering radius is greater than or equal to the packing radius, and when equality is attained the code $\mathcal{C}$ is said to be perfect. As there are only finitely many classes of linear perfect codes, of particular interest are those codes

[1] This research is supported by Norwegian Research Coucil

with $\varrho = e + 1$, called quasi-perfect codes. It is readily seen that any code with covering radius 1 and minimum distance 1 or 2 is quasi-perfect. Therefore, quasi-perfect codes with covering radius 2 and 3 were of more interest and have been extensively studied. Many infinite families of binary, ternary, and quaternary quasi-perfect codes are found (see [9, 11] and references therein).

Let m be a positive integer and π be a primitive element of the field $\mathbb{F}_{p^m}$. For a function f from $\mathbb{F}_{p^m}$ to itself with $f(0) = 0$, define a matrix

$$H_f = \left[\begin{array}{ccccc} 1 & \pi & \pi^2 & \cdots & \pi^{p^m-2} \\ f(1) & f(\pi) & f(\pi^2) & \cdots & f(\pi^{p^m-2}) \end{array} \right],$$

where each symbol stands for the column of its coordinate with respect to a basis of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^m}$. Let $\mathcal{C}_f$ denote the linear code admitting H_f for parity-check matrix.

A function f from $\mathbb{F}_{2^m}$ to itself is called almost perfect nonlinear (APN) if for any $a \in \mathbb{F}_{2^m}^*$, the derivative $D_af(x) = f(x+a)+f(x)$ is 2-to-1, and is referred to as almost bent (AB) if for every $u, v \in \mathbb{F}_{2^m}, u \neq 0$, the extended Walsh transform $W_f(u, v) = \sum_{x\in\mathbb{F}_2^m}(-1)^{tr(uf(x))+tr(vx)}$ equals to 0 or $\pm 2^{\frac{m+1}{2}}$ (m is odd), where $tr(x) = x+x^2+x^4+\cdots+x^{2^{m-1}}$. Every AB function is APN [8], but the converse is not true. A comprehensive survey on APN and AB functions can be found in [6].

Carlet et al in [7] intensively studied the relationship between the APNness and ABness of the function f and the properties of the related code $\mathcal{C}_f$.

Lemma 1. *[7] Let f be a mapping from $\mathbb{F}_{2^m}$ to itself with $f(0) = 0$. Then, f is APN if and only if the linear code $\mathcal{C}_f$ has minimum distance* 5*. Moreover, for $m \geq 3$, if f is APN, then the linear code $\mathcal{C}_f$ has dimension* $2^m - 1 - 2m$*.*

There is an interesting connection between AB functions and the uniformly packed codes, whose covering radius equals to its external distance (i.e., the number of different nonzero distances between the codewords of its dual).

Lemma 2. *[7] Let f be a mapping from $\mathbb{F}_{2^m}$ to itself with $f(0) = 0$. Then, f is AB if and only if the linear code $\mathcal{C}_f$ is a uniformly packed code with the minimum distance* 5 *and covering radius* 3*.*

2 Binary quasi-perfect linear codes from APN quadratic functions

Recall that $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called quadratic if, up to addition of a constant function,

$$f(x) = \sum_{i,j=0}^{m-1} a_{i,j}x^{2^i+2^j},\ a_{i,j} \in \mathbb{F}_{2^m}. \qquad (1)$$

In the m odd case, any quadratic function is APN if and only if it is AB [7]. This fact combined with Lemma 2 implies that every quadratic APN function on odd variables gives a uniformly packed code $\mathcal{C}_f$ with minimum distance 5 and covering radius 3.

By applying the divisibility property of number of solutions of a system of certain polynomial equations, Moreno and Castro in [13] showed that the linear code $\mathcal{C}_f$ with $f(x) = x^{2^i+1}$, $(i, m) = 1$ has covering radius 3.

In what follows, we will investigate the covering radius of $\mathcal{C}_f$ for general quadratic APN functions in a direct way. It will be shown that for quadratic functions f with $f(0) = 0$, f is APN if and only if the corresponding code $\mathcal{C}_f$ is quasi-perfect.

Proposition 1. *Let f be a mapping from $\mathbb{F}_{2^m}$ to itself with $f(0) = 0$. If the linear code $\mathcal{C}_f$ is quasi-perfect, then f is APN.*

Proof. As proved in [7], for any mapping f, the minimum distance of $\mathcal{C}_f$ satisfies $3 \leq d \leq 5$, where $d \geq 3$ comes from the fact every two columns of H_f are distinct and $d \leq 5$ is derived from the non-existence of a linear code $[2^m - 1, k, d]$ for $k \geq 2^m - 1 - 2m$ and $d \geq 6$. Thus, the linear code $\mathcal{C}_f$ has packing radius $1 \leq e \leq 2$. On the other hand, for any $\alpha \neq 0$, there exists no element $x, y \in \mathbb{F}_{2^m}^*$ satisfying

$$\begin{cases} x + y = 0 \\ f(x) + f(y) = \alpha. \end{cases}$$

This together with $f(0) = 0$ implies that the covering radius of $\mathcal{C}_f$ is at least 3. Hence, if the linear code $\mathcal{C}_f$ is quasi-perfect, then its minimum distance must be 5. It follows from Lemma 1 that f is an APN function. □

For quadratic APN functions, as aforementioned, the code $\mathcal{C}_f$ for odd m has covering radius 3. The following proposition settles the covering radius of $\mathcal{C}_f$ for any positive integer m.

Proposition 2. *Let f be a quadratic function as given in (1). For $m \geq 3$, if f is APN, then the linear codes $\mathcal{C}_f$ has covering radius* 3.

Proof. By Definition 1, we need to show that for any $(\alpha, \beta) \in \mathbb{F}_{2^m}^2$, there exist $x_1, x_2, x_3 \in \mathbb{F}_{2^m}$ satisfying

$$\begin{aligned} x_1 + x_2 + x_3 &= \alpha \\ f(x_1) + f(x_2) + f(x_3) &= \beta. \end{aligned} \tag{2}$$

Let $N(\alpha, \beta)$ denote the number of solutions x_1, x_2, x_3 of (2).

Taking $y_t = x_t + \alpha$ for $t = 1, 2, 3$, we have

$$\begin{aligned} f(y_t) &= \sum_{i,j=0}^{m-1} a_{i,j}(x_t + \alpha)^{2^i+2^j} \\ &= \sum_{i,j=0}^{m-1} a_{i,j}(x_t^{2^i+2^j} + \alpha^{2^i} x_t^{2^j} + \alpha^{2^j} x_t^{2^i} + \alpha^{2^i+2^j}). \end{aligned}$$

Then, since $x_1 + x_2 + x_3 = \alpha$, it follows that

$$\begin{aligned} & f(y_1) + f(y_2) + f(y_3) \\ = & \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_2^{2^i+2^j} + x_3^{2^i+2^j}) + \sum_{i,j=0}^{m-1} a_{i,j}\alpha^{2^i}(x_1^{2^j} + x_2^{2^j} + x_3^{2^j}) \\ & + \sum_{i,j=0}^{m-1} a_{i,j}\alpha^{2^j}(x_1^{2^i} + x_2^{2^i} + x_3^{2^i}) + \sum_{i,j=0}^{m-1} a_{i,j}\alpha^{2^i+2^j} \\ = & \sum_{i,j=0}^{m-1} a_{i,j}(x_1^{2^i+2^j} + x_2^{2^i+2^j} + x_3^{2^i+2^j}) + f(\alpha). \end{aligned}$$

Thus, the elements x_1, x_2, x_3 satisfying (2) if and only if y_1, y_2, y_3 satisfy

$$\begin{aligned} y_1 + y_2 + y_3 &= 0 \\ f(y_1) + f(y_2) + f(y_3) &= \beta', \end{aligned} \tag{3}$$

where $\beta' = \beta + f(\alpha)$. That is to say, $N(\alpha, \beta) = N(0, \beta')$.

We next show $N(0, \gamma) \geq 1$ for any $\gamma \in \mathbb{F}_{2^m}^*$ if f is APN.

Following from the definition, it is easily seen that f is APN if and only if $f(x_1)+f(x_2)+f(x_3)+f(x_1+x_2+x_3) = 0$ can be achieved only when $x_1 = x_2$ or $x_1 = x_3$ or $x_2 = x_3$. By an observation in [6] attributed to Dillon, if $f(x)$ is APN, then for any nonzero $\gamma \in \mathbb{F}_{2^m}^*$, the equation $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = \gamma$ has at least a solution. Indeed, suppose there exists a nonzero element γ_0 not contained in the set $\{f(x_1)+f(x_2)+f(x_3)+f(x_1+x_2+x_3) : x_1, x_2, x_3 \in \mathbb{F}_{2^m}\}$, then for any Boolean function $\varphi : \mathbb{F}_{2^m} \to \mathbb{F}_2$, the function $f'(x) = f(x) + \gamma_0\varphi(x)$ will be APN. This is because the equation

$$f'(x_1) + f'(x_2) + f'(x_3) + f'(x_1 + x_2 + x_3) = 0$$

suggests

$$f(x_1)+f(x_2)+f(x_3)+f(x_1+x_2+x_3) = (\varphi(x_1)+\varphi(x_2)+\varphi(x_3)+\varphi(x_1+x_2+x_3))\gamma_0,$$

and then one has $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 + x_3) = 0$. The APNness of f implies that $f(x_1)+f(x_2)+f(x_3)+f(x_1+x_2+x_3) = 0$ can be achieved only when $x_1 = x_2$ or $x_1 = x_3$ or $x_2 = x_3$. Thus, $f'(x_1)+f'(x_2)+f'(x_3)+f'(x_1+x_2+x_3) = 0$ is achieved only when $x_1 = x_2$ or $x_1 = x_3$ or $x_2 = x_3$ as well, and then $f'(x)$ is APN.

Furthermore, if we take $\varphi(x) = tr(\delta_0 f(x))$ with $tr(\delta_0\gamma_0) = 1$, then

$$tr(\delta_0 f'(x)) = tr(\delta_0 f(x) + \delta_0\gamma_0\varphi(x)) = tr(\delta_0 f(x)) + tr(\delta_0\gamma_0)\varphi(x) = 0. \tag{4}$$

¿From Lemma 1, the linear code $\mathcal{C}_{f'}$ defined from the APN function f' has dimension $2^m - 1 - 2m$. That is to say, $tr(\delta_0 f'(x)) = 0$ holds only when $\delta_0 = 0$. This is a contradiction. Hence, the equation $f(x_1) + f(x_2) + f(x_3) + f(x_1 + x_2 +$

$x_3) = \gamma$ has at least a solution. This is equivalent to saying that for any $\gamma \in \mathbb{F}_{2^m}^*$, the system

$$\begin{array}{rcl} x_1 + x_2 + x_3 & = & x_4 \\ f(x_1) + f(x_2) + f(x_3) & = & f(x_4) + \gamma \end{array}$$

has at least a solution. Putting $y_t = x_t + x_4$ for $t = 1, 2, 3$, then

$$\begin{array}{rcl} y_1 + y_2 + y_3 & = & 0 \\ f(y_1) + f(y_2) + f(y_3) & = & \gamma \end{array}$$

has at least a solution. That is, $N(0, \gamma) \geq 1$. The proof follows. □

By Propositions 1 and 2, we immediately have

Theorem 1. *For $m \geq 3$ and the quadratic function*

$$f(x) = \sum_{i,j=0}^{m-1} a_{i,j} x^{2^i + 2^j},\ a_{i,j} \in \mathbb{F}_{2^m},$$

the linear code $\mathcal{C}_f$ is quasi-perfect if and only if f is APN.

New constructions of APN functions, which are extended affine (EA) inequivalent and Carlet-Charpin-Zinoviev (CCZ) inequivalent to the known ones are of particular interest [6]. Six classes of APN monomial functions x^d have been found and one class of them, the Gold monomial x^{2^i+1}, $(i, m) = 1$, is quadratic. Dobbertin conjectured that the list of APN monomial functions is complete. Much work has been done as well on quadratic functions to get new APN functions EA/CCZ inequivalent to the known ones, and many infinite classes have been obtained (see [1–5, 10]).

For quadratic APN functions in odd variables, the related codes $\mathcal{C}_f$ are uniformly packed codes with covering radius 3 [7]. Nevertheless, a glance at the list of the currently known quadratic APN functions in [6] shows that a majority of them are APN only in even variables. In this paper, all these functions in even variables are shown to yield linear codes with minimum distance 5 and covering radius 3. Further study on the extended Walsh spectrum of quadratic functions in even variables reveals that the generated quasi-perfect codes can not be uniformly packed.

References

[1] C. Bracken, E. Byrne, N. Markin, G. McGuire, An infinite family of quadratic quadrinomial APN functions. http://arxiv.org/pdf/0804. 4799, 2008.

[2] C. Bracken, E. Byrne, N. Markin, G. McGuire, New families of quadratic almost perfect nonlinear trinomials and multinomials, *Finite Fields and their Applications* 14, 2008, 703-714.

[3] L. Budaghyan, C. Carlet, Classes of quadratic APN trinomials and hexanomials and related structures, *IEEE Trans. Inform. Theory* 54, no. 5, 2008, 2354-2357.

[4] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inform. Theory* 54, no. 9, 2008, 4218-4229.

[5] L. Budaghyan, C. Carlet, G. Leander, Constructing new APN functions from known ones, *Finite Fields and Their Applications* 15, no. 2, 2009, 150-159.

[6] C. Carlet, Vectorial (multi-output) boolean functions for cryptography, in *Boolean Methods and Models, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press.* Preliminary version available at: *http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html.*

[7] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* 15, 1998, 125-156.

[8] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, in Advances in Cryptology, Eurocrypt'94 (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1995, vol. 950, 356-365.

[9] G. Cohen, M. Karpovsky, F. Mattson, J. Schatz, Covering radius – survey and recent results, *IEEE Trans. Inform. Theory* 31, no. 3, 1985, 328-343.

[10] Y. Edel, G. Kyureghyan, A. Pott, A new APN function which is not equivalent to a power mapping, *IEEE Trans. Inform. Theory* 52, no. 2, 2006, 744-747.

[11] T. Etzion, B. Mounits, Quasi-perfect codes with small distance, *IEEE Trans. Inform. Theory* 51, no. 11, 2005, 3938-3946.

[12] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, *IEEE Trans. Inform. Theory* 14, 1968, 154-156.

[13] O. Moreno, F. Castro, Divisibility properties for covering radius of certain cyclic codes, *IEEE Trans. Inform. Theory* 49, no. 12, 2003, 3299-3303.