On quadratic APN functions $F(x) + \mathrm{Tr}(x)L(x)$

Hiroaki Taniguchi[1*]

[1*]Department of Education, Yamato University, 2-5-1, Katayamacho, Suita City, 564-0082, Japan.

Corresponding author(s). E-mail(s): taniguchi.hiroaki@yamato-u.ac.jp;

Abstract

We first characterize how two $(n-1,m)$ functions f and g can be combined into an APN (n,m)-function F of the form $F(x) = f(x)$ and $F(x+e_0) = g(x)$ for $x \in \mathbb{F}_2^{n-1}$ with $e_0 \in \mathbb{F}_2^n \backslash \mathbb{F}_2^{n-1}$. Next we specialize this cahracterization to the case when f is quadratic and $g(x) = f(x)+L(x)$ for some linearized polynomial L. Lastly for a qudratic APN (n,n)-function F and a linearized polynomial L, we give a characterization of APN-ness for (n,n)-function $F(x) + \mathrm{Tr}(x)L(x)$. With some computational experiments, we see that CCZ-inequivalent APN functions $F(x)+\mathrm{Tr}(x)L(x)$ can be obtained from F using this construction.

1 Preliminaries

Let $\mathbb{F}_2$ be the binary field, and n, m positive integers. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an almost perfect nonlinear (APN) function if the cardinality $|\{x \mid F(x+a)+F(x) = b\}|$ is less than or equal to 2 for any nonzero $a \in \mathbb{F}_2^n$ and for any $b \in \mathbb{F}_2^m$. APN functions have been studied for many years because of their applications in cryptography. See [1], [2] or [5] for known APN functions. We call a function F *quadratic* if $F(x+y)+F(x)+F(y)+F(0)$ is $\mathbb{F}_2$-bilinear. Two functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called *CCZ-equivalent* if the graphs $G_{F_1} := \{(x, F_1(x)) \mid x \in \mathbb{F}_2^n\}$ and $G_{F_2} := \{(x, F_2(x)) \mid x \in \mathbb{F}_2^n\}$ in $\mathbb{F}_2^n \oplus \mathbb{F}_2^m$ are affine equivalent, that is, if there exists an $\mathbb{F}_2$-linear isomorphism $l \in GL_2(\mathbb{F}_2^n \oplus \mathbb{F}_2^m)$ and an element $v \in \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ such that $l(G_{F_1}) + v = G_{F_2}$. *The* Γ*-rank* of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the rank of the incidence matrix over

$\mathbb{F}_2$ of the incidence structure $\{\mathcal{P}, \mathcal{B}, I\}$, where $\mathcal{P} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$, $\mathcal{B} = \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ and $(a, b)I(u, v)$ for $(a, b) \in \mathcal{P}$ and $(u, v) \in \mathcal{B}$ if and only if $F(a+u) = b+v$. We know that if two functions F_1 and F_2 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are CCZ-equivalent, then they have the same Γ-rank (see [3]). Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. We sometimes identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ as an $\mathbb{F}_2$-vector space. We denote the set $\mathbb{F}_{2^n}\backslash\{0\}$ by $\mathbb{F}_{2^n}^\times$ and $\mathbb{F}_2^n\backslash\{0\}$ by $(\mathbb{F}_2^n)^\times$. For finite fields $K \supset F$ of characteristic 2, we denote the trace function from K to F by Tr_F^K. We denote $\mathrm{Tr}_{\mathbb{F}_2}^K$ by Tr and call it the absolute trace of K.

For a function F on $\mathbb{F}_{2^n}$, the value at $a \in \mathbb{F}_{2^n}$ of the Walsh transformation of the Boolean function $\mathbb{F}_{2^n} \ni x \mapsto \mathrm{Tr}(bF(x)) \in \mathbb{F}_2$ for $b \in \mathbb{F}_{2^n}^\times$ is defined by

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

The Walsh spectrum of F is defined by $\mathcal{W}_F = \{W_F(a, b) \mid a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\times\}$. For a quadratic APN function F on $\mathbb{F}_{2^n}$, it is known that $W_F \in \{0, \pm 2^{(n+1)/2}\}$ if n is odd. For the case n is even, it is said that a quadratic APN function F has the classical Walsh spectrum if $\mathcal{W}_F = \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$, and F has the non-classical Walsh spectrum if otherwise (see [4]).

2 A condition to have an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ using APN functions f, g from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$

Let f, g be functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$. We regard $\mathbb{F}_2^{n-1} \subset \mathbb{F}_2^n$ as an F_2-linear subspace. Let $e_0 \in \mathbb{F}_2^n$ with $e_0 \notin \mathbb{F}_2^{n-1}$ and $\mathbb{F}_2^{n-1} + e_0 := \{x + e_0 \mid x \in \mathbb{F}_2^{n-1}\}$. Then $\mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0)$. , We want to have an APN function F from $\mathbb{F}_2^n = \mathbb{F}_2^{n-1} \cup (\mathbb{F}_2^{n-1} + e_0)$ to $\mathbb{F}_2^m$ defined by $F(x) = f(x)$ and $F(x + e_0) = g(x)$ for $x \in \mathbb{F}_2^{n-1}$.

Proposition 1 *F defined above is an APN function if and only if*

(1) *f and g are APN functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$,*
(2) *$f(x+a) + f(x) \neq g(y+a) + g(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$ and for any nonzero $a \in \mathbb{F}_2^{n-1}$, and*
(3) *$G_a : \mathbb{F}_2^{n-1} \ni x \mapsto f(x+a) + g(x) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.*

Proof Recall that F is an APN function if and only if, for any nonzero $A \in \mathbb{F}_2^n$ and for $X, Y \in \mathbb{F}_2^n$, $F(X+A) + F(X) = F(Y+A) + F(Y)$ implies $X = Y$ or $X = Y + A$.

Firstly assume that F is an APN function, and we will see that f and g must satisfy the conditions (1), (2) and (3).

Let $A = a \in (\mathbb{F}_2^{n-1})^\times$. For any $Y = y \in \mathbb{F}_2^{n-1}$, we must have $X = y \in \mathbb{F}_2^{n-1}$ or $X = y + a \in \mathbb{F}_2^{n-1}$ from $F(X+a) + F(X) = F(y+a) + F(y)$. Since $X \in \mathbb{F}_2^{n-1}$, we have $f(X+a)+f(X) = f(y+a)+f(y)$ from $F(X+a)+F(X) = F(y+a)+F(y)$. Thus f must be an APN function. Next, for any $Y = y+e_0$ with $y \in \mathbb{F}_2^{n-1}$ we must have $X = y+e_0$ or $X = y+a+e_0$ from $F(X+a)+F(X) = F(y+e_0+a)+F(y+e_0)$. Since $X = x+e_0$ for some $x \in \mathbb{F}_2^{n-1}$, we have $g(x+a)+g(x) = g(y+a)+g(y)$ from $F(X+a)+F(X) = F(y+e_0+a)+F(y+e_0)$. Hence g must be an APN function. Thus the condition (1) must be satisfied.

Let $A = a \in (\mathbb{F}_2^{n-1})^\times$. For any $Y = y \in \mathbb{F}_2^{n-1}$, since $X = y$ or $X = y+a$, $F(X+a)+F(X) = F(y+a)+F(y)$ does not have a solution $X = x+e_0$ for $x \in \mathbb{F}_2^{n-1}$. Thus $F(x+e_0+a)+F(x+e_0) \neq F(y+a)+F(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$, therefore we must have $g(x+a)+g(x) \neq f(y+a)+f(y)$ for any $x, y \in \mathbb{F}_2^{n-1}$. Thus the condition (2) must be satisfied.

Let $A = a+e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y \in \mathbb{F}_2^{n-1}$. We have $X = y \in \mathbb{F}_2^{n-1}$ or $X = y+a+e_0$ with $y+a \in \mathbb{F}_2^{n-1}$. For $X \in \mathbb{F}_2^{n-1}$, we have $g(X+a)+f(X) = g(y+a)+f(y)$ from $F(X+a+e_0)+F(X) = F(y+a+e_0)+F(y)$, hence $g(X+a)+f(X) = g(y+a)+f(y)$ must have only one solution $X = y$ for any $y, a \in \mathbb{F}_2^{n-1}$. For $X \notin \mathbb{F}_2^{n-1}$, we have $f(X+a)+g(X) = g(y+a)+f(y)$ from $F(X+a)+F(X+e_0) = F(y+a+e_0)+F(y)$, hence $f(X+a)+g(X) = g(y+a)+f(y)$ must have only one solution $X = y+a$. Thus we see that the condition (3) must be satisfied.

Conversely, let us assume the conditions (1), (2) and (3). Assume $F(X+A)+F(X) = F(Y+A)+F(Y)$ with $A \neq 0$. We will prove that $X = Y$ or $X = Y+A$. We divide the case into the following four cases (i) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y \in \mathbb{F}_2^{n-1}$, (ii) $A = a \in (\mathbb{F}_2^{n-1})^\times$ and $Y = y+e_0$ with $y \in \mathbb{F}_2^{n-1}$, (iii) $A = a+e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y$ with $y \in \mathbb{F}_2^{n-1}$, and (iv) $A = a+e_0$ with $a \in \mathbb{F}_2^{n-1}$ and $Y = y+e_0$ with $y \in \mathbb{F}_2^{n-1}$.

Firstly let us consider the case (i). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $f(x+a)+f(x) = f(y+a)+f(y)$ hence $x = y$ or $x = y+a$ by (1). Let $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+g(x) = f(y+a)+f(y)$ which has no solution by (2). Therefore, $X = Y$ or $X = Y+A$ in case (i).

Next, we consider the case (ii). Assume $X = x \in \mathbb{F}_2^{n-1}$, then we have $f(x+a)+f(x) = g(y+a)+g(y)$ which has no solution by (2). If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+g(x) = g(y+a)+g(y)$, hence $x+e_0 = y+e_0$ or $x+e_0 = y+e_0+a$ by (1). Thus we have $X = Y$ or $X = Y+A$ in case (ii).

Let us consider the case (iii). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x) = g(y+a)+f(y)$. Since $G_a : x+a \mapsto f(x)+g(x+a)$ is a one-to-one mapping by (3), we have $x = y$. If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $f(x+a)+g(x) = g(y+a)+f(y)$. By the same reason as above, we have $x+e_0 = y+(a+e_0)$. Thus we have $X = Y$ or $X = Y+A$ in case (iii).

Lastly we consider the case (iv). If $X = x \in \mathbb{F}_2^{n-1}$, then we have $g(x+a)+f(x) = f(y+a)+g(y)$. Since $G_a : x \mapsto f(x+a)+g(x)$ is a one-to-one mapping by (3), we have $x = (y+e_0)+(a+e_0)$. If $X = x+e_0$ with $x \in \mathbb{F}_2^{n-1}$, then we have $f(x+a)+g(x) = f(y+a)+g(y)$. By the same reason as above, we have $x+e_0 = y+e_0$. Thus we also have $X = Y$ or $X = Y+A$ in case (iv).

Hence F must be an APN function under the conditions (1), (2) and (3). $\square$

3 The case f is a quadratic APN function and $g(x) = f(x) + L'(x)$ with L' a linear mapping

Let f be a function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$ and $B_f(x,a) := f(x+a)+f(x)+f(a)+f(0)$. Recall that f is quadratic if $B_f(x,a)$ is an $\mathbb{F}_2$-bilinear mapping. In this section, we consider the case that f is a quadratic APN function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, and $g(x) = f(x)+L'(x)$ for $x \in \mathbb{F}_2^{n-1}$ with L' an $\mathbb{F}_2$-linear mappings from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$. We note that, if f is quadratic, $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x)+B_f(x,a) \in \mathbb{F}_2^m$ are linear mappings for any $a \in \mathbb{F}_2^{n-1}$. We check the conditions (1), (2) and (3) in Proposition 1. We regard $\mathbb{F}_2^{n-1}$ as an $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$.

Proposition 2 *Let f be a quadratic APN function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$, and $g(x) = f(x)+L'(x)$ with L' an $\mathbb{F}_2$-linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^m$. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ defined in Section 2, that is, $F(x) := f(x)$ and $F(x+e_0) := f(x)+L'(x)$ for some fixed $e_0 \in \mathbb{F}_2^n \backslash \mathbb{F}_2^{n-1}$ for $x \in \mathbb{F}_2^{n-1}$. Then F is an APN function if and only if $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x)+B_f(x,a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$.*

Proof Since f and $g = f + L'$ are APN functions, the condition (1) is satisfied. The condition (2) implies $f(x+a)+f(x) \neq f(y+a)+f(y)+L'(a)$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, that is, $L'(a) + (f(x+a)+f(x)) + (f(y+a)+f(y)) \neq 0$ for any $x, y \in \mathbb{F}_2^{n-1}$ if $a \neq 0$, which means $L'(a)+B_f(a, x+y) \neq 0$ if $a \neq 0$, $a \in \mathbb{F}_2^{n-1}$. The condition (3) implies $G_a : \mathbb{F}_2^{n-1} \ni x \mapsto f(x+a)+g(x) = L'(x)+(f(x+a)+f(x)) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$, that is, $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x)+B_f(x,a)+f(a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$. Thus we see that the conditions (1), (2) and (3) in Proposition 1 are satisfied if and only if $\mathbb{F}_2^{n-1} \ni x \mapsto L'(x)+B_f(x,a) \in \mathbb{F}_2^m$ are one-to-one mappings for any $a \in \mathbb{F}_2^{n-1}$. $\square$

4 $F(x) + \mathrm{Tr}(x)L(x)$ for a quadratic APN function F on $\mathbb{F}_{2^n}$

Let $T_0 := \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}(x) = 0\}$ and $e_0 \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ and $B_F(x,a) := F(x+a)+F(x)+F(a)+F(0)$ for $x, a \in \mathbb{F}_{2^n}$. Let L be an $\mathbb{F}_2$-linear mapping on $\mathbb{F}_{2^n}$.

Theorem 3 *Let F be a quadratic APN function on $\mathbb{F}_{2^n}$ and L an $\mathbb{F}_2$-linear mapping on $\mathbb{F}_{2^n}$. Let $e_0 \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Then, $F(x)+\mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a : T_0 \ni x \mapsto L(x)+B_F(x, a+e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$. (Hence, $F(x)+\mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if, and only if, $L_a(x) = 0$ implies $x = 0$ for any $a \in T_0$).*

Proof Let $f := F|_{T_0}$ be the restriction of F to T_0; f is a quadratic APN function from T_0 to $\mathbb{F}_{2^n}$. For $x \in T_0$, we have $F(x)+\mathrm{Tr}(x)L(x) = f(x)$ and $F(x+e_0)+$

$\mathrm{Tr}(x+e_0)L(x+e_0) = f(x)+L(x)+B_F(x,e_0)+L(e_0)+F(e_0)$. Let G be a function on $\mathbb{F}_{2^n}$ defined by $G(x) := f(x)$ and $G(x+e_0) := f(x) + L(x) + B_F(e_0, x)$ for $x \in T_0$, then $G(x) = F(x) + \mathrm{Tr}(x)(L(x) + L(e_0) + F(e_0))$ for $x \in \mathbb{F}_{2^n}$, which is CCZ equivalent to $F(x)+\mathrm{Tr}(x)L(x)$. By Proposition 2, G is an APN function if and only if $T_0 \ni x \mapsto L(x) + B_F(x,e_0) + B_F(x,a) \in \mathbb{F}_{2^n}$ are one-to-one mappings for any $a \in T_0$. Thus $F(x) + \mathrm{Tr}(x)L(x)$ is a quadratic APN function on $\mathbb{F}_{2^n}$ if and only if $L_a : T_0 \ni x \mapsto L(x) + B_F(x, a+e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$. $\square$

Let e_0 be some fixed element of $\mathbb{F}_{2^n}$ with $\mathrm{Tr}(e_0) = 1$. Using a computer, for linear mappings L on $\mathbb{F}_{2^n}$ such that $L_a : T_0 \ni x \mapsto L(x) + B(x, a + e_0) \in \mathbb{F}_{2^n}$ are one-to-one mappings from T_0 to $\mathbb{F}_{2^n}$ for any $a \in T_0$, we have 448 L's with $L(e_0) = 0$ for $F(x) = x^3$ on $\mathbb{F}_{2^4}$, 4608 L's with $L(e_0) = 0$ for $F(x) = x^3$ on $\mathbb{F}_{2^5}$, and many (about $40,000$) L's with $L(e_0) = 0$ for $F(x) = x^3$ on $\mathbb{F}_{2^6}$.

Example 1 Let $F(x) = x^3$ on $\mathbb{F}_{2^6}$. The Γ-rank of F is 1102. Using a computer, we see that there are linear mappings L satisfying the conditions in Theorem 3 such that the Γ-ranks of $F(x) + \mathrm{Tr}(x)L(x)$ are 1144, 1146, 1158, 1166, 1168, 1170, 1172 and 1174. We also see that $F(x) + \mathrm{Tr}(x)L(x)$ with $L(x) = \alpha^{42}x + \alpha^{19}x^2 + \alpha^{51}x^{2^2} + \alpha^{59}x^{2^3} + \alpha^{26}x^{2^4} + \alpha^{38}x^{2^5}$, where α is a primitive element of $\mathbb{F}_{2^6}$, has non-classical Walsh spectrum $\mathcal{W}_F = \{0, \pm 8, \pm 16, \pm 32\}$ with the Γ-rank 1170. Since $F(x) + \mathrm{Tr}(x)L(x)$ with $L(x) = \alpha^{42}x + \alpha^{47}x^2 + \alpha^{35}x^{2^2} + \alpha^{54}x^{2^3} + \alpha^{23}x^{2^4} + \alpha^{27}x^{2^5}$ has classical Walsh spectrum $\mathcal{W}_F = \{0, \pm 8, \pm 16\}$ with the Γ-rank 1170, we see that there are inequivalent APN functions $F(x) + \mathrm{Tr}(x)L(x)$ with the same Γ-rank.

Let $F(x) = x^3$ on $\mathbb{F}_{2^7}$. The Γ-rank of F is 3610. Using a computer, we find that the linear mapping $L(x) := x + x^{2^3} + x^{2^5} + x^{2^6}$ satisfies the conditions in Theorem 3 and the Γ-rank of $F(x) + \mathrm{Tr}(x)L(x)$ is 4048.

References

[1] M. Calderini, L. Budaghyan and C. Carlet, On known constructions of APN and AB functions and their relation to each other, Proceedings of the 20th Central European Conference on Cryptography, Matematicke znanosti 25, pp. 79–105 (2021).

[2] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge (2021).

[3] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematics of Communications 3, pp. 59–81 (2009).

[4] A. Pott, Almost perfect and planar functions, Designs, Codes and Cryptography 78, pp. 141–195 (2016).

[5] https://boolean.h.uib.no/mediawiki/index.php/ .