Designs, Codes and Cryptography (2019) 87:1973–1983
https://doi.org/10.1007/s10623-018-00598-2

On some quadratic APN functions

Hiroaki Taniguchi[1]

Received: 28 March 2018 / Revised: 14 December 2018 / Accepted: 14 December 2018 /
Published online: 3 January 2019

Abstract
A construction of APN functions using the bent function $B(x, y) = xy$ is proposed in Carlet (Des Codes Cryptogr 59:89–109, 2011). At this time, two families of APN functions using this construction are known, that is, the family of Carlet (2011) and the family of Zhou and Pott (Adv Math 234:43–60, 2013). In this note, we propose another family of APN functions with this construction, which are not CCZ equivalent to the former two families on $\mathbb{F}_{2^8}$. We also propose a family of presemifields and determined the middle, left, right nuclei and the center of the associated semifields.

Keywords APN function · Semifield · Projective polynomial

Mathematics Subject Classification 11T71 · 06E30 · 12K10 · 51A35

1 Introduction

Let m, n be positive integers. Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements, and denote by $\mathbb{F}_{2^n}^{\times}$ its multiplicative group. For any finite set S, we denote by $|S|$ the cardinality of S. A function F on $\mathbb{F}_2^m$ is called an APN function if F satisfies $|\{x \in \mathbb{F}_2^m \mid F(x+a)+F(x) = b\}| \leq 2$ for any non-zero $a \in \mathbb{F}_2^m$ and any $b \in \mathbb{F}_2^m$. We call F a quadratic function if $F(x+y)+F(x)+F(y)+F(0)$ is $\mathbb{F}_2$-bilinear for any $x, y \in \mathbb{F}_2^m$. Two functions F_1 and F_2 on $\mathbb{F}_2^m$ are called CCZ equivalent if the graphs $G_{F_1} := \{(x, F_1(x)) \mid x \in \mathbb{F}_2^m\}$ and $G_{F_2} := \{(x, F_2(x)) \mid x \in \mathbb{F}_2^m\}$ in $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are affine equivalent, that is, if there exists a $\mathbb{F}_2$-linear isomorphism $L \in GL_2(\mathbb{F}_2^m \times \mathbb{F}_2^m)$ and an element $v \in \mathbb{F}_2^m \times \mathbb{F}_2^m$ such that $L(G_{F_1}) + v = G_{F_2}$. A Γ-rank of a function F on $\mathbb{F}_2^m$ is the rank of the incidence matrix over $\mathbb{F}_2$ of an incidence structure $\{\mathcal{P}, \mathcal{B}, I\}$, where $\mathcal{P} = \mathbb{F}_2^m \times \mathbb{F}_2^m$, $\mathcal{B} = \mathbb{F}_2^m \times \mathbb{F}_2^m$ and $(a, b)I(u, v)$ for $(a, b) \in \mathcal{P}$ and $(u, v) \in \mathcal{B}$ if and only if $F(a + u) = b + v$.

Proposition 1 (Edel–Pott [11]) *If two functions F_1 and F_2 on $\mathbb{F}_2^m$ are CCZ equivalent, then they have the same Γ-ranks.*

Communicated by T. Helleseth.

✉ Hiroaki Taniguchi
taniguchi@t.kagawa-nct.ac.jp

[1] National Institute of Technology, Kagawa College, 355, Chokushicho, Takamatsu, Kagawa 761-8058, Japan

In this note, we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^{2n}$ with $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ as $\mathbb{F}_2$-vector spaces, and consider the APN function F on $\mathbb{F}_2^{2n}$ with the following form:

$$F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \ni (x, y) \mapsto (xy, G(x, y)) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}. \tag{1}$$

APN functions of this type were first considered by Carlet in [9]. The conditions on G such that F is an APN function are given by Carlet in 4.2.1 of [9]. If F is quadratic, these conditions are as follows:

1. $\mathbb{F}_{2^n} \ni x \mapsto G(x, y) \in \mathbb{F}_{2^n}$ is an APN function for every $y \in \mathbb{F}_{2^n}$,
2. $\mathbb{F}_{2^n} \ni y \mapsto G(x, y) \in \mathbb{F}_{2^n}$ is an APN function for every $x \in \mathbb{F}_{2^n}$, and
3. $\mathbb{F}_{2^n} \ni x \mapsto G(x, \alpha x) \in \mathbb{F}_{2^n}$ is an APN function for every $\alpha \in \mathbb{F}_{2^n}^\times$.

2 Known examples and their Γ-ranks in $\mathbb{F}_{2^8}$

For two positive integers m, n, the greatest common divisor of them is denoted by $GCD(m, n)$. So far, only two examples of APN functions of the form (1) are known.

Theorem 1 (Carlet [9]) *Let n be an integer with $n \geq 2$, i, j integers such that $GCD(n, i - j) = 1$. Let $s, t, u, v \in \mathbb{F}_{2^n}$ with $s \neq 0$, $t \neq 0$. Set $G(x, y) = sx^{2^i+2^j} + ux^{2^i} y^{2^j} + vx^{2^j} y^{2^i} + ty^{2^i+2^j}$. Then $F(x, y) := (xy, G(x, y))$ is an APN function if and only if the polynomial $G(x, 1) = sx^{2^i+2^j} + ux^{2^i} + vx^{2^j} + t$ has no root in $\mathbb{F}_{2^n}$.*

Theorem 2 (Zhou–Pott [15]) *Let m, n be positive integers with $n \geq 2$ and $GCD(m, n) = 1$. Let $\alpha \in \mathbb{F}_{2^n}^\times$ and $\sigma \in Gal(\mathbb{F}_{2^n}/\mathbb{F}_2)$, the Galois group of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $G(x, y) = x^{2^m+1} + \alpha y^{(2^m+1)\sigma}$. Then $F(x, y) := (xy, G(x, y))$ is an APN function if and only if $\alpha \notin \{a^{2^m+1}(t^{2^m} + t)^{1-\sigma} \mid a, t \in \mathbb{F}_{2^n}\}$.*

Corollary 1 (Zhou–Pott [15]) *Let m, n be positive integers with $n \geq 2$ even and $GCD(m, n) = 1$. Let $\alpha \in \mathbb{F}_{2^n}^\times$ and set $G(x, y) = x^{2^m+1} + \alpha y^{(2^m+1)2^i}$. If α is non-cubic (i.e., $\alpha \neq t^3$ for any $t \in \mathbb{F}_{2^n}$) and i is even, $F(x, y) := (xy, G(x, y))$ is an APN function.*

In case $i = 0$, or σ is an identity mapping, Theorem 2 and Corollary 1 are covered by Theorem 1.

Lemma 1 *Let F be a function and L a $\mathbb{F}_2$-linear function, both defined on $\mathbb{F}_{2^n}$. Then F and $F + L$ are CCZ equivalent.*

Proof We sometimes denote $L(x)$ by xL, which means the linear operator L acts on x. Then in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, we see $(x, F(x)) \begin{pmatrix} 1 & L \\ 0 & 1 \end{pmatrix} = (x, F(x) + xL) = (x, F(x) + L(x))$. □

The following corollary may be well known.

Corollary 2 *The APN functions in Theorem 1 are CCZ equivalent to $F'(x, y) = (xy, G'(x, y))$ with $G'(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$, where $m = i - j$, $a \in \{0, 1\}$ and some $b \in \mathbb{F}_{2^n}^\times$, such that the polynomial $G(x, 1) = x^{2^m+1} + ax + b$ has no root in $\mathbb{F}_{2^n}$.*

Proof By the coordinate change $(x, y) \mapsto (x, \lambda x + y)$ for some $\lambda \in \mathbb{F}_{2^n}$, we can eliminate u, that is, we have $F(x, y) = (xy + \lambda x^2, G_1(x, y))$, where $G_1(x, y) = s'x^{2^i+2^j} + v'x^{2^j} y^{2^i} + t'y^{2^i+2^j}$ with $s', v', t' \in \mathbb{F}_{2^n}$, $s', t' \neq 0$. Next, by the linear transformation $\Phi_1 : (u, v) \mapsto$

$(u, (v/s')^{2^{-j}})$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, we have $\Phi_1(F(x, y)) = (xy + \lambda x^2, G_2(x, y))$ with $G_2(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$, where $m = i - j$ and $a, b \in \mathbb{F}_{2^n}$ with $b \neq 0$. If $a = 0$, we have established the statement if we set $G' := G_2$, since $\Phi_1(F(x, y)) = (xy + \lambda x^2, G'(x, y))$ is CCZ equivalent to $F'(x, y) = (xy, G'(x, y))$ by Lemma 1.

Let $a \neq 0$. By the coordinate change $(x, y) \mapsto (a^{2^{-m}}x, y)$ followed by the linear transformation $\Phi_2 : (u, v) \mapsto ((1/a^{2^{-m}})u, (1/a^{2^{-m}+1})v)$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, we have $\Phi_2(\Phi_1(F(x, y))) = (xy + \lambda' x^2, G'(x, y))$ for some λ' with $G'(x, y) = x^{2^m+1} + xy^{2^m} + b'y^{2^m+1}$ for some $b' \neq 0$. We set $b := b'$. Then we have established the statement for the case $a \neq 0$, since $\Phi_2(\Phi_1(F(x, y))) = (xy+\lambda' x^2, G'(x, y))$ is CCZ equivalent to $F'(x, y) = (xy, G'(x, y))$ by Lemma 1. Note that, in both cases $a = 0$ and $a = 1$, the polynomial $G'(x, 1) = x^{2^m+1}+ax+b$ has no root in $\mathbb{F}_{2^n}$ by assumption on $G(x, 1)$. □

We have the following fact by Helleseth and Kholosha.

Fact 1 (Theorem. 1 of [12]) *For a positive integer $m < n$ with $GCD(m, n) = 1$, the number of $b \in \mathbb{F}_{2^n}^{\times}$ such that the polynomial $x^{2^m+1} + x + b$ has no root in $\mathbb{F}_{2^n}$ is $(2^n + 1)/3$ if n is odd, and $(2^n - 1)/3$ if n is even.*

Hence there are many polynomials $x^{2^m+1} + ax + b$ as in Corollary 2 which have no root in $\mathbb{F}_{2^n}$. As for the constant term $b \in \mathbb{F}_{2^n}^{\times}$ with n even such that the equation $x^{2^m+1} + x + b = 0$ with $GCD(m, n) = 1$ has no root in $\mathbb{F}_{2^n}$, interesting and useful results are proved in [7].

The Γ-ranks of the APN functions F' in Corollary 2 on $\mathbb{F}_{2^8}$, which equal the Γ-ranks of the APN functions F in Theorem 1 on $\mathbb{F}_{2^8}$ by Proposition 1 and Corollary 2, are calculated using Magma [6]. They are all 13,200, which is the Γ-rank of the function $x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48}$ in the Table 10, 2.1 of [11].

As for the functions F in Corollary 1 by Y. Zhou and A. Pott, there are the cases $m = 1$ or $m = 3$, and $i = 0$ or $i = 2$ on $\mathbb{F}_{2^8}$. According to Zhou–Pott [15], the Γ-rank is 13,200 if $i = 0$ (in this case F belongs to the family of Theorem 1). On the other hand, the Γ-rank is 13,642 if $i = 2$. Thus, on $\mathbb{F}_{2^8}$, the APN functions in Corollary 1 with $i = 2$ and the APN functions in Theorem 1 are CCZ inequivalent.

3 Another example

Theorem 3 *Let m, n be positive integers with $n \geq 2$ and $GCD(m, n) = 1$. Let $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^{\times}$. Let us define*

$$G(x, y) = x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1}. \tag{2}$$

Then $F(x, y) := (xy, G(x, y))$ is an APN function if and only if the polynomial $P(x) := x^{2^m+1} + ax + b$ has no root in $\mathbb{F}_{2^n}$.

We note that, if $a = 0$, then $F(x, y)$ in Theorem 3 belongs to the family of Theorem 2. The next theorem is a different expression of Theorem 3. Note that Theorem 3 is obtained from Theorem 4 by the substitution $x \mapsto x^{2^{2m}}$.

Theorem 4 *Let m, n be positive integers with $n \geq 2$ and $GCD(m, n) = 1$. Let $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^{\times}$. Let us define $G(x, y) = x^{2^m+1} + axy^{2^m} + by^{2^m+1}$. Then*

$$F(x, y) := (x^{\tau}y, G(x, y))$$

with $x^{\tau} := x^{2^{-2m}}$, is an APN function if and only if the polynomial $G(x, 1) := x^{2^m+1}+ax+b$ has no root in $\mathbb{F}_{2^n}$.

Using the expression of $G(x, y)$ in Theorem 4 and using the same method as in the proof of Corollary 2, we have the following proposition.

Proposition 2 *The function $F(x, y) = (xy, G(x, y))$ in Theorem 3 is CCZ equivalent to the function $F'(x, y) = (xy, G'(x, y))$, where $G'(x, y) = x^{2^{2m}+2^{3m}} + a'x^{2^{2m}}y^{2^m} + b'y^{2^m+1}$ for some a', b' with $a' \in \{0, 1\}$ and $b' \in \mathbb{F}_{2^n}^\times$. Moreover, F' is APN if and only if $P'(x) = x^{2^m+1} + a'x + b'$ has no root in $\mathbb{F}_{2^n}$.*

We omit the proof because it is a copy of the proof of Corollary 2.

Proof of Theorem 3 We have to check the conditions 1,2,3 of Section 1 by Carlet. (See the last paragraph of Section 1 of this article.) The conditions 1 and 2 are clearly satisfied. We have to investigate on the condition 3. Since $G(x, \alpha x) = x^{2^{2m}+2^{3m}} + a\alpha^{2^m}x^{2^{2m}+2^m} + b\alpha^{2^m+1}x^{2^m+1}$, we see that $G(x, \alpha x)$ is the composition mapping of the Gold function $z := g(x) = x^{2^m+1}$ and the linear mapping $L_\alpha(z) = z^{2^{2m}} + a\alpha^{2^m}z^{2^m} + b\alpha^{2^m+1}z$. Hence, we see that $G(x, \alpha x)$ is an APN function if $L_\alpha(z)$ is an injective mapping on $\mathbb{F}_{2^n}$, that is, the polynomial $L_\alpha(z)$ has no root other than $z = 0$. Since $b \neq 0$ by assumption, we see that $L_\alpha(z)$ has no root other than $z = 0$ if and only if the polynomial $L_\alpha(z)/z = z^{2^{2m}-1} + a\alpha^{2^m}z^{2^m-1} + b\alpha^{2^m+1}$ has no root in $\mathbb{F}_{2^n}$. Let $s := z^{2^m-1}$. Then we see that this condition is equivalent to the condition that $L_\alpha(z)/(\alpha^{2^m+1}z) = (s/\alpha)^{2^m+1} + a(s/\alpha) + b$ has no root in $\mathbb{F}_{2^n}$. Lastly, let $t := s/\alpha$, then we see that $G(x, \alpha x)$ is an APN function if the polynomial $P(t) := L_\alpha(z)/(\alpha^{2^m+1}z) = t^{2^m+1} + at + b$ has no root in $\mathbb{F}_{2^n}$. Now, assume to the contrary that $P(t)$ has a non-zero root t in $\mathbb{F}_{2^n}$. Then $L_\alpha(z)$ has a non-zero root $z = (\alpha t)^{1/(2^m-1)}$. Since $\alpha \mapsto (\alpha t)^{1/(2^m-1)}$ is a permutation on $\mathbb{F}_{2^n}^\times$ for a fixed root $t \neq 0$ and since $g(x) = x^{2^m+1}$ is a Gold function, there exist $a \in \mathbb{F}_{2^n}^\times$, $b' \in \mathbb{F}_{2^n}$ and $\alpha \in \mathbb{F}_{2^n}^\times$ such that the two equations $g(x+a)+g(x) = b'$ and $g(x+a)+g(x) = b'+(\alpha t)^{1/(2^m-1)}$ have solutions. Let $b := L_\alpha(b')$. Then we have $b = L_\alpha(b' + (\alpha t)^{1/(2^m-1)})$ by definitions of t and α. Let x_1 and x_2 be solutions of $g(x + a) + g(x) = b'$ and $g(x + a) + g(x) = b' + (\alpha t)^{1/(2^m-1)}$ respectively, then $x_1 + a$ and $x_2 + a$ are also solutions of them. Recall $G(x + a, \alpha(x + a)) + G(x, \alpha x) = L_\alpha(g(x+a)+g(x))$ with $g(x) = x^{2^m+1}$. Then, from $G(x+a, \alpha(x+a))+G(x, \alpha x) = b$, we have $g(x+a)+g(x) = b'$ and $g(x+a)+g(x) = b'+(\alpha t)^{1/(2^m-1)}$. Hence we have more than four solutions x_1, x_1+a, x_2 and x_2+a for the equation $G(x+a, \alpha(x+a))+G(x, \alpha x) = b$. Thus $G(x, \alpha x)$ is not an APN function for some $\alpha \in \mathbb{F}_{2^n}^\times$ if we assume that $P(t)$ has a non-zero root t in $\mathbb{F}_{2^n}$. □

We have calculated the Γ-ranks of the APN functions in Theorem 3 under the conditions that $a \neq 0$ using Magma [6]. We obtained that the Γ-rank is 13,700 if $b^5 = 1$, and the Γ-rank is 13,798 if $b^5 \neq 1$. If $a = 0$, the Γ-rank is 13,642, since APN functions (2) are in a family of Corollary 1 with $i = 2$ if $a = 0$. Therefore, we see that the family in Theorem 3 has more than two CCZ equivalent classes on $\mathbb{F}_{2^8}$. We notice that the Γ-ranks 13,700 and 13,798 of the APN functions in Theorem 3 do not appear in the list by Edel and Pott [11], or the list by Budaghyan et al. [8] arising from the known infinite families of APN functions, which means the function is also not equivalent to other known families such as the Gold or the Budaghyan–Carlet–Leander functions.

APN functions	Γ-ranks in $\mathbb{F}_{2^8}$
Theorem 1 [Carlet]	13,200
Corollary 1 with $i = 2$ [Zhou–Pott]	13,642
Theorem 3 with $a \neq 0$ and $b^5 = 1$	13,700
Theorem 3 with $a \neq 0$ and $b^5 \neq 1$	13,798

4 Related presemifields on $\mathbb{F}_{p^n}$

Let p be a prime number. Let $F := \mathbb{F}_{p^n}$ be the finite field of p^n elements. The polynomial $ax^{p^m+1} + bx^{p^m} + cx + d \in F[x]$ with $a \neq 0$ is called a projective polynomial. A recent reference is Bluher [5]. Let K be a subfield of F with $|K| \geq 3$. Let σ be a generator of the Galois group $Gal(F/K)$ of F over K. Let $a, b \in F$ and $P(x) := x^{\sigma+1} + ax + b$. Note that $P(x)$ is a projective polynomial. We assume that the equation $P(x) = 0$ has no root in F. Let α be a non-zero element in F with the norm $N_K^F(-\alpha) \neq 1$. Let us define a multiplication $x \circ_\alpha y := x^\sigma y + \alpha x y^\sigma$, which is the multiplication of the twisted presemifield of Albert [1].

Lemma 2 *If $x \circ_\alpha y = 0$, then $x = 0$ or $y = 0$.*

Proof Let $x \neq 0$ and $y \neq 0$, and assume that $x \circ_\alpha y = 0$. Then from $x^\sigma y + \alpha x y^\sigma = 0$ we have $(x/y)^\sigma/(x/y) = -\alpha$. Thus we have a contradiction since the norm of the left hand side is 1, and the norm of the right hand side is not equal to 1 by assumption on α. □

We need the following lemma.

Lemma 3 *If the projective polynomial $P(x) = x^{\sigma+1} + ax + b$ above satisfies $P(x) \neq 0$ for all $x \in F$, then the linear mapping $L_\beta : F \to F$ defined by $L_\beta(x) := x^{\sigma^2} + a\beta^\sigma x^\sigma + b\beta^{\sigma+1}x$ is invertible for any non-zero $\beta \in F$.*

Proof Assume to the contradiction that $L_\beta(z) = 0$ for some non-zero $z \in F$. Since $z \neq 0$, we have $z^{\sigma^2-1} + a\beta^\sigma z^{\sigma-1} + b\beta^{\sigma-1} = 0$. Let us put $X := z^{\sigma-1}$. Then we have $X^{\sigma+1} + a\beta^\sigma X + b\beta^{\sigma+1} = 0$. Note that $X \neq 0$ since $z \neq 0$ and $X = z^\sigma/z$. Next we divide both sides of the equation by $\beta^{\sigma+1}$ and put $Y := X/\beta$. Then $Y^{\sigma+1} + aY + b = 0$ with $Y \neq 0$. Thus we have $P(Y) = 0$ with $Y \neq 0$, which contradicts to the assumption that $P(x) \neq 0$ for all $x \in F$. □

Theorem 5 *Let $(x, s), (y, t) \in F \times F$. We define a multiplication $*$ on $F \times F$ as follows. Then we have a presemifield $(F \times F, +, *)$.*

$$(x, s) * (y, t) := ((x \circ_\alpha y)^{\sigma^2} - a(x^\sigma t - \alpha y^\sigma s)^\sigma - b(s \circ_\alpha t), xt + ys). \tag{3}$$

We notice that, if $a = 0$, p is odd, $\alpha = 1$ and the extension degree $[F : K]$ is odd, this presemifield is a member of the presemifields in Theorem 1 of [15].

Proof It is clear that the multiplication $(x, s) * (y, t)$ is additive on both (x, s) and (y, t). Now assume that $(x, s) * (y, t) = (0, 0)$. Then we have to prove that, if $(x, s) \neq (0, 0)$ then $(y, t) = (0, 0)$, and if $(y, t) \neq (0, 0)$ then $(x, s) = (0, 0)$. We only give the proof of the first case, since we are able to give the similar proof for the second case.

Firstly, let $s = 0$, then $x \neq 0$ since $(x, s) \neq (0, 0)$, thus we have $t = 0$ from the second equation $xt + ys = 0$ of (3). Therefore, we have $x \circ_\alpha y = 0$ from the first equation of (3)

and hence we have $y = 0$ by Lemma 2. Thus we have proved that $(y, t) = (0, 0)$. By the same way, we have $(y, t) = (0, 0)$ if $x = 0$.

Next, we will prove that $(y, t) = (0, 0)$ under the conditions $(x, s) * (y, t) = (0, 0)$ with $x \neq 0$ and $s \neq 0$. We assume to the contradiction that $(y, t) \neq (0, 0)$. From this assumption, we must have $y \neq 0$ and $t \neq 0$ by the second equation $xt + ys = 0$ of (3). Since $xt + ys = 0$ with $x, y, s, t \neq 0$, there exists a non-zero $\beta \in F$ such that $s/x = -t/y = \beta$. Let us substitute s by βx, and t by $-\beta y$ on the first equation of (3). Then we have $(x \circ_\alpha y)^{\sigma^2} + a\beta^\sigma (x \circ_\alpha y)^\sigma + b\beta^{\sigma+1}(x \circ_\alpha y) = 0$. Let us put $z := x \circ_\alpha y$, then we have $z^{\sigma^2} + a\beta^\sigma z^\sigma + b\beta^{\sigma+1} z = 0$. Recall that $z \neq 0$ by the assumption that $x \neq 0$, $y \neq 0$ and by Lemma 2. Thus we have a contradiction since $L_\beta(z) = z^{\sigma^2} + a\beta^\sigma z^\sigma + b\beta^{\sigma+1} z \neq 0$ by Lemma 3. □

Let $(F \times F, +, \star)$ be the associated semifield of the presemifield $(F \times F, +, *)$ of Theorem 5 with the identity element $(1, 0) * (1, 0)$. Then,

$$((x, s) * (1, 0)) \star ((1, 0) * (y, t)) = (x, s) * (y, t)$$

for any $x, s, y, t \in F$ by Kaplansky's trick (see [13]). As for the definitions of middle, left, right nuclei and the center, we refer to Lavrauw and Polverino [13]. We note that the center C of the semifield is the intersection of the associative center (the intersection of the three nuclei) and the commutative center (consists of the elements which commute with all elements of the semifield). We will prove the following theorem.

Theorem 6 *We assume that the extension degree $[F : K] \geq 3$. Then the middle nucleus N_m is isomorphic to K if $a \neq 0$. The right nucleus N_r and the left nucleus N_l are also isomorphic to K. The commutative center is isomorphic to K if $\alpha \neq 1$ or $a \neq 0$. Hence the center C is isomorphic to K if $a \neq 0$.*

We notice that K is a subfield of N_m, N_l, N_r and C of the semifield $(F \times F, +, \star)$ because of Proposition 3 of [3], since it is easy to check that $(lx, ls) * (y, t) = (x, s) * (ly, lt) = l((x, s) * (y, t))$ for any $l \in K$ and any $x, s, t, y \in F$ for the multiplication $*$ defined by (3) and the field multiplication of F denoted by $l(x, s) = (lx, ly)$. In the case $a = 0$ and $\alpha = 1$ (hence p and $[F : K]$ must be odd since $N_K^F(-\alpha) \neq 1$), the results of Theorem 6 for middle, left and right nuclei follow from Theorem 2(b) and Theorem 3 of [15]. The commutative center is $F \times F$ since the associated semifields are commutative in the case $a = 0$ and $\alpha = 1$ (see [15]). We will prove Theorem 6 using the Propositions 3–6 below, which will be proved in the following part of this article.

Notice that $x \mapsto x^\sigma y + \alpha x y^\sigma$ is an injective mapping for any fixed $y \neq 0$, and $y \mapsto x^\sigma y + \alpha x y^\sigma$ is an injective mapping for any fixed $x \neq 0$. Let $y, t \in F$. Let $y' \in F$ be the unique element determined by

$$(y' + \alpha y'^\sigma)^{\sigma^2} - at^\sigma = (y^\sigma + \alpha y)^{\sigma^2} + a(\alpha t)^\sigma \tag{4}$$

from y and t. Then we easily see that

$$(y, t) * (1, 0) = (1, 0) * (y', t).$$

Let $x, s, y', t \in F$. Let $A \in F$ be an element which satisfies that

$$(A, y's + xt) * (1, 0) = (x, s) * (y', t).$$

Then A is uniquely determined by

$$(A^\sigma + \alpha A)^{\sigma^2} + a(\alpha(y's + xt))^\sigma = (x \circ_\alpha y')^{\sigma^2} - a(x^\sigma t - \alpha y'^\sigma s)^\sigma - b(s \circ_\alpha t). \tag{5}$$

Let $y, t, z, u \in F$. Let $B \in F$ be an element which satisfies that

$$(1,0) * (B, zt + yu) = (y,t) * (z,u).$$

Then B is uniquely determined by

$$(B + \alpha B^{\sigma})^{\sigma^2} - a(zt + yu)^{\sigma} = (y \circ_{\alpha} z)^{\sigma^2} - a(y^{\sigma}u - \alpha z^{\sigma}t)^{\sigma} - b(t \circ_{\alpha} u). \tag{6}$$

Let $X := (x,s) * (1,0)$, $Y := (y,t) * (1,0) = (1,0) * (y',t)$ and $Z := (1,0) * (z,u)$. Let us assume that

$$(X \star Y) \star Z = X \star (Y \star Z). \tag{7}$$

Then we easily see, using Kaplansky's trick (see [13]), that

$$(A, y's + xt) * (z,u) = (x,s) * (B, zt + yu).$$

Thus, from (7), we have the equations:

$$\begin{aligned}&(A \circ_{\alpha} z)^{\sigma^2} - a(A^{\sigma}u - \alpha z^{\sigma}(y's + xt))^{\sigma} - b((y's + xt) \circ_{\alpha} u)\\ &= (x \circ_{\alpha} B)^{\sigma^2} - a(x^{\sigma}(zt + yu) - \alpha B^{\sigma}s)^{\sigma} - b(s \circ_{\alpha} (zt + yu))\end{aligned} \tag{8}$$

and

$$Au + z(y's + xt) = Bs + x(zt + yu). \tag{9}$$

Recall that the extension degree $[F : K] \geq 3$ by assumption, and σ is a generator of the Galois group $Gal(F/K)$. We use the following lemma.

Lemma 4 *Let $a, b, c \in F$ such that $az_i^{\sigma^2} + bz_i^{\sigma} + cz_i = 0$ for some $z_i \in F$, $i = 1, 2, 3$ which are linearly independent over K. Then $a = b = c = 0$.*

Proof See 3.51. Lemma of [14]. □

Proposition 3 *The middle nucleus N_m is isomorphic to K if $a \neq 0$.*

Proof We have to determine $Y = (y,t) * (1,0)$ $(= (1,0) * (y',t))$ if (7) is satisfied for any $X = (x,s) * (1,0)$ and $Z = (1,0) * (z,u)$, i.e., for any $(x,s), (z,u) \in F \times F$. Let $u = 0$ and $s \neq 0$. Then from (9), we have $B = zy'$. Next using (6) with $u = 0$ and $B = zy'$, we have

$$(y'z + \alpha(y'z)^{\sigma})^{\sigma^2} - a(zt)^{\sigma} = (y \circ_{\alpha} z)^{\sigma^2} + a(\alpha z^{\sigma}t)^{\sigma}.$$

Thus we have

$$(\alpha^{\sigma^2}y^{\sigma^2} - \alpha^{\sigma^2}y'^{\sigma^3})z^{\sigma^3} + (y^{\sigma^3} + a\alpha^{\sigma}t^{\sigma} - y'^{\sigma^2})z^{\sigma^2} + at^{\sigma}z^{\sigma} = 0$$

for any $z \in F$. Then by Lemma 4, we have $t = 0$ since $a \neq 0$, and $y'^{\sigma} = y$, $y^{\sigma} = y'$, hence $y^{\sigma^2} = y$, for (y,t) with $Y = (y,t) * (1,0) = (1,0) * (y',t) \in N_m$. Let $u = 0$ and $s \neq 0$. Then we have $B = zy' = zy^{\sigma}$ by (9) as above. By (8) with $u = 0$, and using $t = 0$, $y' = y^{\sigma}$, we have

$$(A \circ_{\alpha} z)^{\sigma^2} + a(\alpha z^{\sigma}y^{\sigma}s)^{\sigma} = (x^{\sigma}y^{\sigma}z + \alpha xyz^{\sigma})^{\sigma^2} + a(\alpha yz^{\sigma}s)^{\sigma}.$$

Thus we have

$$(\alpha^{\sigma^2}A^{\sigma^2} - \alpha^{\sigma^2}x^{\sigma^2}y)z^{\sigma^3} + (A^{\sigma^3} + a\alpha^{\sigma}ys^{\sigma} - x^{\sigma^3}y^{\sigma} - a\alpha^{\sigma}y^{\sigma}s^{\sigma})z^{\sigma^2} = 0.$$

We notice that A is determined only by y, t, x, s by the Eq. (5) and independent of z, u. Then we have $A^{\sigma^2} = x^{\sigma^2} y$ and $a\alpha^{\sigma}(y - y^{\sigma})s^{\sigma} = 0$. Thus we have $y^{\sigma} = y$, i.e., $y \in K$ if $a \neq 0$. Therefore we must have $Y = (y, 0) * (1, 0)$ with $y \in K$. Hence N_m is isomorphic to K if $a \neq 0$. □

Proposition 4 *The left nucleus N_l is isomorphic to K.*

Proof We have to determine $X = (x, s) * (1, 0)$ if (7) is satisfied for any $Y = (y, t) * (1, 0) = (1, 0) * (y', t)$ and $Z = (1, 0) * (z, u)$ with $y, y', t, z, u \in F$. Firstly, we assume that $s \neq 0$ to the contradiction. Let $u = 0$. Then from (9), we have $B = zy'$. Next using (6) with $u = 0$ and $B = zy'$, we have

$$(y'z + \alpha(y'z)^{\sigma})^{\sigma^2} - a(zt)^{\sigma} = (y \circ_{\alpha} z)^{\sigma^2} + a(\alpha z^{\sigma} t)^{\sigma}.$$

This equation holds for any $z \in F$. Notice that y, y', t are independent of z. From this equation, we have

$$(\alpha^{\sigma^2} y^{\sigma^2} - \alpha^{\sigma^2} y'^{\sigma^3})z^{\sigma^3} + (y^{\sigma^3} + a\alpha^{\sigma} t^{\sigma} - y'^{\sigma^2})z^{\sigma^2} + at^{\sigma} z^{\sigma} = 0$$

for any $z \in F$. Then by Lemma 4, we have $y'^{\sigma} = y$, $y^{\sigma} = y'$ (and $t = 0$ if $a \neq 0$). Thus we must have $y^{\sigma^2} = y$ if $s \neq 0$. However, since y, t are any element in F and $[F : K] \geq 3$, we have a contradiction if $s \neq 0$. Therefore, we must have $s = 0$ if $X = (x, s) * (1, 0) \in N_l$. Since $s = 0$, we have $A = xy$ from (9) if $u \neq 0$. Let $u \neq 0$ and $t = 0$. Then by (4) we have

$$y' + \alpha y'^{\sigma} = y^{\sigma} + \alpha y.$$

By (5), we have

$$x^{\sigma} y' + \alpha x y'^{\sigma} = x^{\sigma} y^{\sigma} + \alpha x y.$$

Thus we have

$$y' - y^{\sigma} = \alpha(y - y'^{\sigma}) \text{ and } x^{\sigma}(y' - y^{\sigma}) = \alpha x(y - y'^{\sigma}). \tag{10}$$

We note that, if $y - y'^{\sigma} = 0$ or $y' - y^{\sigma} = 0$ then $y^{\sigma^2} = y$ by (10). However, there exists $y \in F$ such that $y^{\sigma^2} \neq y$ since $[F : K] \geq 3$. Using this y, we have

$$x^{\sigma}(y' - y^{\sigma}) = x(y' - y^{\sigma})$$

with $y' - y^{\sigma} \neq 0$ by (10). Therefore, we must have $x^{\sigma} = x$. Thus we have $X = (x, 0) * (1, 0)$ with $x \in K$. Hence N_l is isomorphic to K. □

Proposition 5 *The right nucleus N_r is isomorphic to K.*

Proof We have to determine $Z = (1, 0) * (z, u)$ if (7) is satisfied for any $X = (x, s) * (1, 0)$ and $Y = (y, t) * (1, 0) = (1, 0) * (y', t)$ with $x, u, y, y', t \in F$. Firstly, we assume that $u \neq 0$ to the contradiction. Let $s = 0$. Then from (9), we have $A = xy$. Next using (5) with $s = 0$ and $A = xy$, we have

$$((xy)^{\sigma} + \alpha xy)^{\sigma^2} + a(\alpha x t)^{\sigma} = (x \circ_{\alpha} y')^{\sigma^2} - a(x^{\sigma} t)^{\sigma}.$$

This equation holds for any $x \in F$. Notice that y, y', t are independent of x. Thus we have

$$x^{\sigma^3}(y^{\sigma^3} - y'^{\sigma^2}) + x^{\sigma^2}(\alpha^{\sigma^2} y^{\sigma^2} - \alpha^{\sigma^2} y'^{\sigma^3} - at^{\sigma}) + x^{\sigma}(a\alpha^{\sigma} t^{\sigma}) = 0$$

for any $x \in F$. Then by Lemma 4, we have $y'^{\sigma} = y$, $y^{\sigma} = y'$ (and $t = 0$ if $a \neq 0$). Thus we must have $y^{\sigma^2} = y$ if $u \neq 0$. However, since y, t are any element in F and $[F : K] \geq 3$, we have a contradiction if $u \neq 0$. Therefore, we must have $u = 0$ if $Z = (1, 0) * (z, u) \in N_r$. Since $u = 0$, we have $B = zy'$ from (9) if $s \neq 0$. Let $s \neq 0$ and $t = 0$. Then by (4), we have

$$y' + \alpha y'^{\sigma} = y^{\sigma} + \alpha y.$$

By (6), we have

$$zy' + \alpha z^{\sigma} y'^{\sigma} = y^{\sigma} z + \alpha y z^{\sigma}.$$

Then by the same method as in the proof of Proposition 4, we have $Z = (1, 0) * (z, 0)$ with $z \in K$. Hence N_r is isomorphic to K. □

Recall that, if $a = 0$ and $\alpha = 1$ (hence p and $[F : K]$ must be odd since $N_K^F(-\alpha) \neq 1$), the presemifield in Theorem 5 belongs to the commutative presemifields of Theorem 1 of Zhou–Pott [15].

Proposition 6 *The commutative center is isomorphic to K if $a \neq 0$ or $\alpha \neq 1$.*

Proof Let $x, s, y, t \in F$. Let $x', y' \in F$ be

$$(x, s) * (1, 0) = (1, 0) * (x', s) \text{ and } (y, t) * (1, 0) = (1, 0) * (y', t).$$

Then we have

$$(x' + \alpha x'^{\sigma})^{\sigma^2} - as^{\sigma} = (x^{\sigma} + \alpha x)^{\sigma^2} + a(\alpha s)^{\sigma}, \text{ and} \tag{11}$$

$$(y' + \alpha y'^{\sigma})^{\sigma^2} - at^{\sigma} = (y^{\sigma} + \alpha y)^{\sigma^2} + a(\alpha t)^{\sigma}. \tag{12}$$

Let us assume that $(x, s)*(1, 0)$ is in the commutative center. Then, for any $(y, t) \in F \times F$, we have

$$((y, t) * (1, 0))\star((1, 0) * (x', s)) = ((x, s) * (1, 0))\star((1, 0) * (y', t)).$$

By Kaplansky's trick, we have

$$(y, t) * (x', s) = (x, s) * (y', t) \tag{13}$$

for any $(y, t) \in F \times F$. We will prove that $x = x' \in K$ and $s = 0$. It follows from (13) that

$$\begin{aligned} &(y \circ_{\alpha} x')^{\sigma^2} - a(y^{\sigma} s - \alpha x'^{\sigma} t)^{\sigma} - b(t \circ_{\alpha} s) \\ &\quad = (x \circ_{\alpha} y')^{\sigma^2} - a(x^{\sigma} t - \alpha y'^{\sigma} s)^{\sigma} - b(s \circ_{\alpha} t), \text{ and} \end{aligned} \tag{14}$$

$$x't + ys = xt + y's. \tag{15}$$

We easily see that, if $x = x' \in K$ and $s = 0$, then (14) and (15) are both satisfied for any $y, t \in F$ because of (12).

Firstly, assume that $\alpha \neq 1$. We assume that $s \neq 0$ to the contradiction. Let $t = 0$. Then we have $y = y'$ by (15). Using $y = y'$ and $t = 0$, we have $y + \alpha y^{\sigma} = y^{\sigma} + \alpha y$ by (12). Hence we have $y - y^{\sigma} = \alpha(y - y^{\sigma})$. However, since $\alpha \neq 1$, we must have $y^{\sigma} = y$. Thus we have a contradiction since y is an arbitrary element in F and $[F : K] \geq 3$. Therefore we must have $s = 0$. Next let $t \neq 0$. Then $x = x'$ by (15). It follows from (11) and $s = 0$, $x = x'$ that $x + \alpha x^{\sigma} = x^{\sigma} + \alpha x$. Thus we have $x^{\sigma} = x$ since $\alpha \neq 1$ by assumption.

Next, assume that $\alpha = 1$ and $a \neq 0$. We recall that p and $[F : K]$ must be odd since $N_K^F(-\alpha) \neq 1$. Let $t = 0$. Then we have $y = y'$ by (12) and $\alpha = 1$. Since $y = y', \alpha = 1$ and $t = 0$, it follows from (14) that

$$(x'^{\sigma^2} - x^{\sigma^2})y^{\sigma^3} + (x'^{\sigma^3} - x^{\sigma^3} + 2as^{\sigma})y^{\sigma^2} = 0.$$

Since y is an arbitrary element in F and $[F : K] \geq 3$, we have $x = x'$ and $s = 0$. Next we calculate (14) – (12) $\times x^{\sigma^2}$ using $x = x', s = 0$ and $\alpha = 1$. Then we have

$$(y - y')^{\sigma^2}(x^{\sigma^3} - x^{\sigma^2}) = 0.$$

We note that $y \neq y'$ if $t \neq 0$ by (12) and $a \neq 0, \alpha = 1$. Hence we must have $x^{\sigma^3} - x^{\sigma^2} = 0$, that is, $x \in K$. Thus we see that, if $(x, s) * (1, 0)$ is an element in the commutative center, we must have $x \in K$ and $s = 0$. Therefore the commutative center is isomorphic to K. □

In [3], Corollary 3, the middle nucleus N_m of the semifield associated to the presemifield $B(p, m, s, l, C_1, C_2)$, p odd, $l \neq 0$, is determined as a quadratic extension of the center (in a quadratic extension of F which is isomorphic to $F \times F$ as F-vector spaces) under some conditions on C_1, C_2, and conjectured that N_m is always a quadratic extension of the center if $l \neq 0$. In [2], Theorem 9, the middle nucleus N_m of the semifield associated to the presemifield $B(2, m, s, l, t)$, $s > 0$, $l \neq 0$ is a quadratic extension of the center. Therefore, under some conditions, the semifield associated to the presemifield $B(p, m, s, l, t)$ in Definition 1 of [4] with p odd and $l \neq 0$, or the presemifield $B(2, m, s, l, t)$ in Definition 1 of [2] with $l \neq 0$ are not isotopic to the semifield $(F \times F, +, \star)$ associated to the presemifield $(F \times F, +, *)$ in Theorem 5 of this article. We conjecture that these semifields associated to the presemifields $B(p, m, s, l, t)$ with p any prime and $l \neq 0$, are not isotopic to our semifield $(F \times F, +, \star)$. The semifields $\mathcal{S}(L_1, L_2)$ of type (a) and (b) in Sect. 4 of Dempwolff [10] of size q^{2n} with q an odd prime power and n a positive odd integer, have middle nucleus isomorphic to $\mathbb{F}_q$ and left nucleus isomorphic to $\mathbb{F}_{q^n}$, right nucleus isomorphic to $\mathbb{F}_q$ (type (b)) or $\mathbb{F}_{q^2}$ (type (a)) (see Theorem 4.3 of [10]). So these semifields are not isotopic to our semifield $(F \times F, +, \star)$ if $n > 1$. The semifields $\mathcal{S}(a, r, s, t)$ in Section 4 of Dempwolff [10] of size q^{2n} with q an odd prime power and n a positive odd integer have right nucleus isomorphic to $\mathbb{F}_{q^f}$ with $f = 2 \times GCD(n, r)$ (see Theorem 4.11 of [10]). Hence these semifields are not isotopic to our semifield $(F \times F, +, \star)$ since n is odd and the right nucleus K of $(F \times F, +, \star)$ is a subfield of $\mathbb{F}_{q^n}$.

Acknowledgements The author thanks the referees for many helpful comments and advices.

References

1. Albert A.A.: On non associative division algebras. Trans. Am. Math. Soc. **72**, 292–309 (1952).
2. Bartoli D., Bierbrauer J., Kyureghyan G., Giulietti M., Marcugini S., Pambianco F.: A family of semifields in characteristic 2. J. Algebr. Comb. **45**, 455–473 (2017).
3. Bierbrauer J.: Projective polynomials, a projection construction and a family of semifields. Des. Codes Cryptogr. **79**, 183–200 (2016).
4. Bierbrauer J., Bartoli D., Faina G., Marcugini S., Pambianco F.: A family of semifields in odd characteristic. Des. Codes Cryptogr. **86**, 611–621 (2018).
5. Bluher A.: On $x^{q+1} + ax + b$. Finite Fields Appl. **10**, 285–305 (2004).
6. Bosma W., Cannon J., Playoust C.: The MAGMA algebra system I: the user language. J. Symb. Comput. **24**, 235–265 (1997).
7. Bracken C., Tan C., Tan Y.: On a class of quadratic polynomials with no zeros and its application to APN functions. Finite Fields Appl. **25**, 26–36 (2014).

8. Budaghyan L., Helleseth T., Li N., Sun B.: Some results on the known classes of quadratic APN functions, codes, cryptology and information security. In: Hajji S.E., Nitaj A., Souidi E.M. (eds.) Proceedings of Second International Conference, C2SI 2017, Lecture Notes on Computer Science, 10194, 3–16 (2017).
9. Carlet C.: Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Des. Codes Cryptogr. **59**, 89–109 (2011).
10. Dempwolff U.: More translation planes and semifields from Dembowski-Ostrom polynomials. Des. Codes Cryptogr. **68**, 81–103 (2013).
11. Edel Y., Pott A.: A new perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**, 59–81 (2009).
12. Helleseth T., Kholosha A.: On the equation $x^{2^l+1} + x + a = 0$ over $GF(2^k)$. Finite Fields Appl. **14**, 159–176 (2008).
13. Lavrauw M., Polverino O.: Finite semifields. In: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry, pp. 131–160. Nova Science Publishers, Inc, New York (2011).
14. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20, 2nd edn. Cambridge University Press, Cambridge (1996).
15. Zhou Y., Pott A.: A new family of semifields with 2 parameters. Adv. Math. **234**, 43–60 (2013).