k-idempotent Bent functions in Partial Spread class

Ziran Tu[*], Claude Carlet[†], Xiangyong Zeng[‡], Xibo Zhang

Abstract: Idempotent functions are an important class of Boolean functions, related to cryptography and coding theory. This paper investigates k-idempotent functions, a natural generalization of idempotent functions. Based on two classes of Dillon-type bent functions proposed in the paper "New characterizations of Dillon-like hyperbent functions via Dickson polynomials", by Z. Tu, C. Li, X. Zeng, T. Helleseth and N. Li, 02 October 2025, Volume 38, article number 35, in Journal of Cryptology, we establish the existence of k-idempotent bent functions (that are not l-idempotents for $l < k$) from the finite field $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ in the partial spread class. More precisely, for any divisor k of n with $k \geq 3$, it is demonstrated that there are k-idempotent bent functions. For $k = 1, 2$, complete characterizations on the k-idempotent bent conditions are provided via the 2-adic orders of integers. The key problem reduces to solving a specific linear equation and computing certain values of the trace function associated with its solutions, which is closely connected to computing the Walsh transform of the Gold functions. By reformulating the target equation into a system of two linear equations and applying trace map properties, the trace is explicitly computed and thus the k-idempotent property is verified.

Keywords: Bent function, k-idempotent function, rotation symmetric Boolean function, partial spread class, trace function.

[*]Z. Tu and X. Zhang are with the Key Laboratory of Intelligent Sensing System and Security (Hubei University), Ministry of Education and Hubei Provincial Engineering Research Center of Intelligent Connected Vehicle Network Security, School of Cyber Science and Technology, Hubei University, Wuhan, 430062, China. Emails: tuziran@aliyun.com, Zhangxb1104@163.com

[†]C. Carlet is with the Universities of Paris 8, Saint-Denis, France and Bergen, Norway. Email: claude.carlet@gmail.com

[‡]X. Zeng (corresponding author) is with the Key Laboratory of Intelligent Sensing System and Security (Hubei University), Ministry of Education and the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan, 430062, China. Email: xiangyongzeng@aliyun.com

1 Introduction

For a positive integer n, let $\mathbb{F}_{2^n}$ denote a finite field of order 2^n and let $\mathbb{F}_2^n$ denote the n-dimensional vector space over $\mathbb{F}_2$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. In the former case, an appropriate representation is the multivariate representation, also called the algebraic normal form, and in the latter case, we generally use the univariate or bivariate representation, which can be expressed by means of the trace function (see [3]). Due to the important applications in symmetric cryptography (see e.g. [1, 3]), combinatorics (see e.g. [8]) and error correcting codes (see e.g. [3, 26]), Boolean functions with desired properties have been a research focus in the past five decades.

Nonlinearity (the minimum Hamming distance between a given Boolean function and all affine Boolean functions) is an important parameter of Boolean functions; thus high nonlinearity is a main criterion for their design. Rothaus [31] had the intuition in the seventies of its role in cryptography, which was confirmed later by the inventions of fast correlation attacks on stream ciphers and linear attacks on block ciphers. Those functions in an even number n of variables that attain the maximum nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ are called bent functions [31]. Since the 1970s, significant research efforts have been devoted to these functions, leading to numerous theoretical advances and practical constructions (see e.g. [3, 6, 7, 9, 14–17, 23–25, 31]). For odd n, bent functions do not exist, while the maximum nonlinearity of n-variable Boolean functions is unknown for $n \geq 9$. The nonlinearity value $2^{n-1} - 2^{\frac{n-1}{2}}$, which is reached by the concatenation of any two $(n-1)$-variable bent functions and by those quadratic Boolean functions whose linear kernel has dimension 1 (see [3] for more details), is known as the bent concatenation bound (a lower bound for the maximum nonlinearity of n-variable Boolean functions). For odd $n \leq 7$, it is known that the maximum nonlinearity is equal to the bent concatenation bound [2, 28], and in 1983, Patterson and Wiedemann constructed 15-variable Boolean functions with nonlinearity exceeding the bent concatenation bound [29]. The 15-variable Patterson-Wiedemann functions belong to in the idempotent class, where a Boolean function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ (which can be represented by its univariate representation) is called an idempotent (or 1-idempotent) if $f(x^2) = f(x)$ for any $x \in \mathbb{F}_{2^n}$.

Like RS (rotation symmetric) functions, the idempotent functions have advantages in terms of storage and computation. They were used by Filiol and Fontaine to construct functions achieving the best possible tradeoffs between some cryptographic fundamental

properties [10, 11]. The concept of RS functions has been naturally generalized to that of k-RS Boolean functions for a positive integer k [13]. Moving back to the univariate representation, any k-RS function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ equals the decomposition over a normal basis $(\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ of $\mathbb{F}_{2^n}$, of what we shall call a k-idempotent function. That is, k is the minimal positive integer such that $f(x) = f(x^{2^k})$ for all $x \in \mathbb{F}_{2^n}$. When $k = 1$, such functions are exactly the idempotents. It should be noted that, while a correspondence exists between RS Boolean functions and idempotents (more generally, between k-RS Boolean functions and k-idempotents), the conversion is computationally complex, which justifies their separate study [4].

A few infinite classes of 1-idempotent bent functions are known in the literature, which, denoting $n = 2m$, are as follows:

1. Quadratic bent functions: $f(x) = c_m \mathrm{Tr}_1^m(x^{2^m+1}) + \sum_{i=1}^{m-1} c_i \mathrm{Tr}_1^n(x^{2^i+1})$ with $c_i \in \mathbb{F}_2$, bent if and only if $\gcd\big(\sum_{i=1}^{m-1} c_i(x^i + x^{n-i}) + c_m x^m,\ x^n + 1\big) = 1$ [20, 35]; more generally, any quadratic bent RS function $g(x_1, x_2, \ldots, x_n)$ yields a bent 1-idempotent $g(x, x^2, \ldots, x^{2^{n-1}})$[4].

2. Niho bent functions: $f(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \mathrm{Tr}_1^n(x^d)$ where $d = s(2^m - 1) + 1$ with $s \in \{3, \frac{1}{4}, \frac{1}{6}\}$ taken modulo $2^m + 1$, and m odd for $s = 1/4$, m even for $s = 1/6$ [9].

3. Leander-Kholosha bent functions: $f(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + \sum_{i=1}^{2^{r-1}-1} \mathrm{Tr}_1^n(x^{d_i})$ with $d_i = \frac{i}{2^r}(2^m - 1) + 1$, $\gcd(r, m) = 1$ [15].

4. Tang et al. construction: $f(x) = \mathrm{Tr}_1^m(x^{2^m+1}) + F(\mathrm{Tr}_1^n(u_1 x), \ldots, \mathrm{Tr}_1^n(u_m x))$ where $\{u_i\}$ is a normal basis and F is a reduced rotation symmetric polynomial [33].

5. Carlet's two constructions: $f_1(xw + yw^2) = \mathrm{Tr}_1^m(x^{2^{(m-1)/2}+1}) + \mathrm{Tr}_1^m(y^{2^{(m-1)/2}+1}) + (\mathrm{Tr}_1^m(x) + \mathrm{Tr}_1^m(x^{2^{(m-1)/2}+1}) + \mathrm{Tr}_1^m(x^3))\,(\mathrm{Tr}_1^m(y) + \mathrm{Tr}_1^m(y^{2^{(m-1)/2}+1}) + \mathrm{Tr}_1^m(y^3)) + \mathrm{Tr}_1^m(x + y)$ for odd m, with $x, y \in \mathbb{F}_{2^m}$ and $w \in \mathbb{F}_4 \setminus \mathbb{F}_2$; and $f_2(x) = \mathrm{Tr}_1^r\big((x + x^{2^{3r}})^{1+2^r+2^{2r}}\big) + \mathrm{Tr}_1^{3r}(x^{1+2^{3r}})$ for $n = 6r$[4].

Dillon's partial spread class of bent functions [8] is one of the main primary constructions of bent functions. For a long time, the partial spreads considered in the literature were mostly subsets of Desarguesian spreads, in relation with the so-called $\mathcal{PS}_{ap}$ class of those bent functions $f(x) = g(x^{2^n-1})$, where $g(0) = 0$ and the restriction of g to the multiplicative subgroup of $\mathbb{F}_{2^{2n}}^*$ of order $2^n + 1$ has Hamming weight 2^{n-1}. Such functions have all their exponents of Dillon-type. It was described in [7, 14] that the generalized

Dillon monomial function $\mathrm{Tr}_1^{2n}(ax^{r(2^n-1)})$ is bent if and only if the Kloosterman sum $\mathcal{K}_n(a)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(x^{-1}+ax)}$ equals 0, where $\gcd(r,2^n+1)=1$ and $a\in\mathbb{F}_{2^n}$. For odd n, Mesnager proved that $\mathrm{Tr}_1^{2n}(ax^{r(2^n-1)})+\mathrm{Tr}_1^2(bx^{\frac{2^{2n}-1}{3}})$ is bent if and only if $\mathcal{K}_n(a)=4$. These two classes of bent functions provide potential 1-idempotents, if $\mathcal{K}_n(1)$ equals 0 or 4. However, as pointed out in [19], the case $\mathcal{K}_n(1)=0$ never happened. Further, it has been checked that the case $\mathcal{K}_n(1)=4$ never happens as well for $5\le n\le 20$ [23]. Thus a natural question arises: Do k-idempotent functions exist in the bent partial spread class? Before this paper, even the existence of 1-idempotent bent functions within the partial spread class was not known. For other small values of k ($k=2$ or 3 for example), no relevant result is available yet to the best of our knowledge.

The authors of [34] investigated the bentness of functions having the form:

$$f_{a,b}^d(x)=\mathrm{Tr}_1^{2n}(a(x^{2^n-1}+b)^d). \tag{1.1}$$

A number of exponents d, as well as the parameters a and b, were identified that make $f_{a,b}^d$ in (1.1) bent. Especially, they proposed two kinds of values for d, belonging to the two sets:

$$\mathcal{D}_1=\left\{-\frac{2^i+3}{2}(2^n-1)-2^i-2:0<i<n\right\},\quad \mathcal{D}_2=\left\{-(2^{i-1}+3)(2^n-1)-2^i-3:2\le i<n\right\}$$

and they characterized the bentness of $f_{a,1}^d$ for $d\in\mathcal{D}=\mathcal{D}_1\cup\mathcal{D}_2$, in terms of the Walsh transform of Gold monomial functions.

The present paper establishes the existence of k-idempotent bent functions in the partial spread class, based on these two classes of Dillon-type bent functions. Our main contributions are:

1. For every divisor k of n with $k\ge 3$, we can choose integers i satisfying $k\mid(i-1)$, along with coefficients a, such that the function $f_{a,1}^d$ (where $d\in\mathcal{D}_2$) is k-idempotent bent.

2. For the cases $k=1,2$, we give explicit conditions on n and i via the 2-adic orders for the k-idempotent bentness of $f_{a,1}^d$ ($d\in\mathcal{D}$).

The core problem reduces to solving a special linear equation

$$y+y^{2^{2i}}+a^{-1}b=0, \tag{1.2}$$

where $a^{-1}b\in\mathbb{F}_{2^{(n,i)}}$ and (n,i) denotes the greatest common divisor of n and i, followed by computing the trace $\mathrm{Tr}_1^n(ay_0^{2^i+1})$ for any solution y_0. Notably, this problem is deeply

connected to the Walsh transform of the Gold functions, which is a nontrivial task, as evidenced by Hou [12]. By reformulating (1.2) as a system of two linear equations, we could write the trace in terms of an intermediate variable θ, and then further proceed the computation by using the transitivity property of trace maps.

The remainder of this paper is organized as follows: Section 2 introduces some necessary preliminaries. Section 3 is divided into two parts: the first part focuses on characterizing a key equality related to the Walsh transform of the Gold monomial functions, while the second part explores the applications in analyzing the k-idempotent properties of two classes of Dillon-type bent functions. Finally, Section 4 concludes the paper.

2 Preliminaries

This section recalls some necessary background in two parts.

2.1 k-idempotent Boolean functions on $\mathbb{F}_{2^n}$

An n-variable Boolean function f is usually defined as a mapping from the vector space $\mathbb{F}_2^n$ to the binary field $\mathbb{F}_2$, and the set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. Since the finite field $\mathbb{F}_{2^n}$ can be identified with the vector space $\mathbb{F}_2^n$ after choosing a basis, a Boolean function $f \in \mathcal{B}_n$ is also treated as a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Recall that for two positive integers m and n with $m \,|\, n$, the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ [18] is defined as

$$\mathrm{Tr}_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}}.$$

Then each non-zero Boolean function $f \in \mathcal{B}_n$ has a unique polynomial representation [23], i.e.,

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{\mathfrak{o}(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1}),\ a_j \in \mathbb{F}_{2^{\mathfrak{o}(j)}}, \tag{2.1}$$

where

- Γ_n denotes the set of integers obtained by choosing exactly one element in each cyclotomic coset modulo $2^n - 1$, including the trivial coset which only contains 0;
- $\mathfrak{o}(j)$ is the size of the coset containing j;
- $\epsilon = wt(f) \pmod 2$.

When regarded as a Boolean function on $\mathbb{F}_{2^n}$, the Walsh transform of f at $\omega \in \mathbb{F}_{2^n}$ becomes

$$W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(\omega x)}.$$

The notion of k-rotation symmetric functions is as follows:

Definition 1 ([32]). *For a positive integer k, a Boolean function $f \in \mathcal{B}_n$ defined on $\mathbb{F}_2^n$ is called k-rotation symmetric (in short, k-RS) if for each input $x \in \mathbb{F}_2^n$, $f(x) = f(\rho_n^k(x))$, where ρ_n^k denotes k-cyclic shift operator, and for any integer $0 < l < k$, there exists at least one vector $x \in \mathbb{F}_2^n$ such that $f(x) \neq f(\rho_n^l(x))$.*

This definition can be naturally extended to k-idempotent functions.

Definition 2. *Let $f \in \mathcal{B}_n$ be defined on $\mathbb{F}_{2^n}$. Then f is called k-idempotent if $f(x) = f(x^{2^k})$ holds for all $x \in \mathbb{F}_{2^n}$, and for any integer $0 < l < k$, there exists at least one element $x \in \mathbb{F}_{2^n}$ such that $f(x) \neq f(x^{2^l})$.*

It is well-known that a function $f \in \mathcal{B}_n$ in univariate polynomial form is 1-idempotent if and only if all its coefficients belong to $\mathbb{F}_2$. A similar characterization of the k-idempotent property, for arbitrary k, in terms of polynomial coefficients is given as follows. (To the best of our knowledge, it has not yet appeared in the literature, although it is easy to prove.)

Proposition 1. *Let $f(x) \in \mathcal{B}_n$ and k be an integer with $k \mid n$. Then $f(x)$ is k-idempotent if and only if all the coefficients in its unique univariate polynomial form lie in $\mathbb{F}_{2^k}$, and for any proper divisor l of k, there exists at least one coefficient that does not belong to $\mathbb{F}_{2^l}$.*

Proof. Recall that each mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ can be represented uniquely as a univariate polynomial in $\mathbb{F}_{2^n}[x]$ under congruence modulo $x^{2^n} - x$. Specifically, we assume that the unique univariate form of $f(x)$ is

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i$$

with $a_i \in \mathbb{F}_{2^n}$. Due to the uniqueness of this representation, we have $(f(x))^{2^k} = f(x^{2^k})$ for all $x \in \mathbb{F}_{2^n}$ if and only if $a_i \in \mathbb{F}_{2^k}$ for all i. Since $f(x)$ is a Boolean function, i.e., $f(x) = (f(x))^2$, which directly implies $f(x) = (f(x))^{2^k}$, we have then $f(x) = f(x^{2^k})$ for all $x \in \mathbb{F}_{2^n}$ if and only if $a_i \in \mathbb{F}_{2^k}$ for all i. The minimality of k in Definition 2 on the k-idempotentness of $f(x)$ proves the proposition. □

However, to our knowledge, no results on k-idempotent functions for general k have appeared in the literature. Currently, the studies focus on the case $k = 1$. In [4], the second author, Gao and Liu introduced a transformation of 1-RS Boolean functions $f(x_0, \ldots, x_{n-1})$ into the 1-idempotent Boolean functions $g(x) = f(x, x^2, \ldots, x^{2^{n-1}})$, having the property that any 1-idempotent Boolean function can be obtained this way. This related a RS Boolean function in multivariate form to an 1-idempotent function in univariate form without using a normal basis, and the computation of this transformation is much less complex than the decomposition/recomposition through a normal basis. Note that the functions $f(x_0, \ldots, x_{n-1})$ and $g(x)$ decomposed over a normal basis are not affine equivalent Boolean functions, in general (that is, there does not exist an affine permutation A such that one equals the other composed on the right by A); in particular, as checked in [4] all cases where f can be bent or not and g can be bent or not do happen. In the same paper, these authors also introduced the bivariate form and established a complete characterization of 1-idempotent functions [4].

2.2 Two classes of Dillon-type Bent functions on $\mathbb{F}_{2^n}$

In this subsection, we revisit the two classes of functions $f_{a,1}^d$ recalled in (1.1) from [34]. According to [34], the bentness of these functions can be characterized by the Walsh transform of Gold monomial functions. For $F(x) = \mathrm{Tr}_1^n(ax^{2^i+1})$, we denote its Walsh transform by

$$\mathcal{G}(i, a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{F(x)+\mathrm{Tr}_1^n(bx)}. \tag{2.2}$$

The two classes of Dillon-type bent functions characterized in [34] are as follows:

Proposition 2. *Let $d = -\frac{2^i+3}{2}(2^n - 1) - 2^i - 2$ and $v_2(n) > v_2(i)$. Let $a \in \mathbb{F}_{2^n}^*$, then $f_{a,1}^d(x)$ is bent if and only if $\mathcal{G}(i, a, 0) = \mathcal{G}(i, a, 1)$.*

Proposition 3. *Let $d = -(2^{i-1} + 3)(2^n - 1) - 2^i - 3$. Then $f_{a,1}^d(x)$ is bent if and only if $\mathcal{G}(i-1, a^{2^{-1}}, a^{2^{-i}}) = \mathcal{G}(i-1, a^{2^{-1}}, a^{2^{-i}} + 1)$ $(i \geq 2)$.*

Observe that these two characterizations are via equalities of the form $\mathcal{G}(j, u, v_1) = \mathcal{G}(j, u, v_2)$. To further determine the k-idempotency of $f_{a,1}^d$, the parameter a needs to be restricted to the subfield $\mathbb{F}_{2^k}$ (see Proposition 1). Consequently, we need to analyze $\mathcal{G}(i, a, b)$ under the condition $a, b \in \mathbb{F}_{2^k}$. As will be detailed in Proposition 4, this analysis reduces to solving Eq.(1.2) when $v_2(n) > v_2(i)$. It is generally nontrivial to determine

the exact value of $\mathcal{G}(i,a,b)$ for explicit $a,b \in \mathbb{F}_{2^n}$, as pointed out by Carlitz and Hou [5, 12]. It is known from [21, Chapter 15] and [3, Proposition 55] that

$$\mathcal{G}(i,a,b) = \eta_{i,a,b} 2^{\frac{n+l(F)}{2}},$$

where $\eta_{i,a,b} \in \{0, \pm 1\}$, and $l(F)$ is the $\mathbb{F}_2$-dimension of $L(F) = \{z \in \mathbb{F}_{2^n} : F(x+z) + F(x) \text{ is a constant}\}$. Thus the key to determining $\mathcal{G}(i,a,b)$ is the computation of $\eta_{i,a,b}$. Utilizing the Jacobi symbol, which is denoted by $J(a,m)$, and defined for $m = \prod_i p_i^{s_i}$ as $J(a,m) = \prod_i L(a,p_i)^{s_i}$, where $L(a,p_i)$ denotes the Legendre symbol, taking value 0 if $a = 0$, value 1 if $a \neq 0$ is a quadratic residue modulo p_i, and value -1 if $a \neq 0$ is a quadratic nonresidue, the coefficients $\eta_{i,a,b}$ were given explicitly below:

Proposition 4 ([12]). *Let $F(x) = \mathrm{Tr}_1^n(ax^{2^i+1})$ with $a \in \mathbb{F}_{2^n}$ and $s = \frac{o(a)}{(o(a),2^i-1)}$, where $o(a)$ denotes the multiplicative order of a and $(o(a), 2^i-1)$ denotes its gcd with 2^i-1. Let $v_2(j)$ denote the 2-adic order of j, i.e., the maximum integer v such that $2^v \mid j$. Then for any $b \in \mathbb{F}_{2^n}$, we have:*

(i) *If $v_2(n) \leq v_2(i)$, then defining $H_{i,a,b}(x) = x^{2^{2i}} + x + \left(\frac{b}{a_1} + 1\right)^{2^i}$ with $a_1 \in \mathbb{F}_{2^n}$ satisfying $a = a_1^{2^i+1}$ and writing $n = 2^e n'$ with n' odd:*

$$\eta_{i,a,b} = \begin{cases} (-1)^{\mathrm{Tr}_1^n(x_0^{2^i+1}+x_0)} J\left(2, \frac{n'}{(n',i)}\right)^{2^e}, & \text{if } H_{i,a,b}(x) = 0 \text{ has a solution } x_0 \in \mathbb{F}_{2^n}, \\ 0, & \text{otherwise.} \end{cases}$$

(ii) *If $v_2(n) > v_2(i)$, then denoting $G_{i,a,b}(x) = ax + a^{2^i} x^{2^{2i}} + b^{2^i}$, then if $G_{i,a,b}(x_0) = 0$ for some x_0, then:*

$$\eta_{i,a,b} = \begin{cases} (-1)^{\mathrm{Tr}_1^n(ax_0^{2^i+1})}, & \text{if } v_2(n) = v_2(i)+1 \text{ and } (2^{2i}-1, \frac{2^n-1}{s}) = 2^{(2i,n)}-1 \\ & \text{or } v_2(n) > v_2(i)+1 \text{ and } (2^{2i}-1, \frac{2^n-1}{s}) \neq 2^{(2i,n)}-1, \\ -(-1)^{\mathrm{Tr}_1^n(ax_0^{2^i+1})}, & \text{if } v_2(n) = v_2(i)+1 \text{ and } (2^{2i}-1, \frac{2^n-1}{s}) \neq 2^{(2i,n)}-1 \\ & \text{or } v_2(n) > v_2(i)+1 \text{ and } (2^{2i}-1, \frac{2^n-1}{s}) = 2^{(2i,n)}-1, \end{cases}$$

and if $G_{i,a,b}(x) = 0$ has no solution in $\mathbb{F}_{2^n}$, then $\eta_{i,a,b} = 0$.

According to Proposition 4, determining the value $\mathcal{G}(i,a,b)$ reduces to solving $H_{i,a,b}(x) = 0$ or $G_{i,a,b}(x) = 0$ and computing the traces involved in the expressions in (i) and (ii), which is not an easy task. When $a,b \in \mathbb{F}_{2^k} \subset \mathbb{F}_{2^{(n,i)}}$, the equation $G_{i,a,b}(x) = 0$ exactly reduces to Eq.(1.2). We note that if $v_2(n) \leq v_2(i)$ and the equation $H_{i,a,b}(x) = 0$ has no

solution in $\mathbb{F}_{2^n}$ (or, respectively, if $v_2(n) > v_2(i)$ and $G_{i,a,b}(x) = 0$ has no solution), then it follows trivially that $\mathcal{G}(i, a, b) = 0$ (due to $\eta_{i,a,b} = 0$). The primary challenge arises when either $H_{i,a,b}(x) = 0$ or $G_{i,a,b}(x) = 0$ admit solutions.

Referring back to Proposition 2, we note that its condition differs slightly from the original version in [34], where only the case $v_2(n) > v_2(i)$ is considered. We point out that in the case $v_2(n) \leq v_2(i)$, it is also possible to give suitable elements a such that $\mathcal{G}(i, a, 1) = \mathcal{G}(i, a, 0)$ (which is fairly easy and not mentioned in [34]) because we just need the equations $H_{i,a,1}(x) = 0$ and $H_{i,a,0}(x) = 0$ have no solution at the same time.

3 Main Results

In this section, we develop a method to partially characterize the sum $\mathcal{G}(i, a, b)$ in (2.2), where the parameters a and b belong to the subfield $\mathbb{F}_{2^{(n,i)}}$. This characterization is then applied to identifying those bent functions in Propositions 2 and 3 that are k-idempotent.

3.1 Partial characterization on the sum $\mathcal{G}(i, a, b)$

Recall that determining the sum $\mathcal{G}(i, a, b)$ is equivalent to determining $\eta_{i,a,b}$. Following the ideas of Proposition 4 by Hou, the next theorem presents a solution for the restricted case that a and b are constrained to the subfield $\mathbb{F}_{2^{(n,i)}}$, giving explicit values for $\eta_{i,a,b}$.

Theorem 1. *Let n and i be two positive integers and $t = (n, i)$. If $a, b \in \mathbb{F}_{2^t} \subset \mathbb{F}_{2^n}$, $a \neq 0$, and $s = \frac{o(a)}{(o(a), 2^i - 1)}$, then $\eta_{i,a,b}$ can take values as follows:*

(1) *if $v_2(n) \leq v_2(i)$, write $n = 2^e n'$ with n' odd, then*

$$\eta_{i,a,b} = \begin{cases} 0, & \text{if } a \neq b^2, \\ J(2, \frac{n'}{(n', i)})^{2^e}, & \text{if } a = b^2; \end{cases}$$

(2) *if $v_2(n) = v_2(i) + 1$, then*

$$\eta_{i,a,b} = \begin{cases} 0, & \text{if } b \neq 0, \\ 1, & \text{if } b = 0 \text{ and } (2^{2i} - 1, \frac{2^n - 1}{s}) = 2^{(2i,n)} - 1, \\ -1, & \text{if } b = 0 \text{ and } (2^{2i} - 1, \frac{2^n - 1}{s}) \neq 2^{(2i,n)} - 1; \end{cases}$$

(3) *if $v_2(n) = v_2(i) + 2$, then*

$$\eta_{i,a,b} = \begin{cases} (-1)^{\mathrm{Tr}_1^t(a^{-1}b^2)}, & \text{if } (2^{2i} - 1, \frac{2^n - 1}{s}) \neq 2^{(2i,n)} - 1, \\ -(-1)^{\mathrm{Tr}_1^t(a^{-1}b^2)}, & \text{if } (2^{2i} - 1, \frac{2^n - 1}{s}) = 2^{(2i,n)} - 1; \end{cases}$$

(4) *if* $v_2(n) > v_2(i) + 2$, *then*

$$\eta_{i,a,b} = \begin{cases} 1, & \text{if } (2^{2i}-1, \frac{2^n-1}{s}) \neq 2^{(2i,n)}-1, \\ -1, & \text{if } (2^{2i}-1, \frac{2^n-1}{s}) = 2^{(2i,n)}-1. \end{cases}$$

Some auxiliary results are necessary to prove Theorem 1. The first is on an affine equation with two linear terms, which is a generalization of the quadratic equation $x^2 + x + a = 0$.

Lemma 1. *Let* $0 < i < n$ *be a positive integer and* $t = (n, i)$. *Then the equation* $x^{2^i} + x + a = 0$ *for* $a \in \mathbb{F}_{2^n}$ *has a solution in* $\mathbb{F}_{2^n}$ *if and only if* $\mathrm{Tr}_t^n(a) = 0$.

Proof. Assume that there exists some x_0 such that $x_0^{2^i} + x_0 + a = 0$. Since $t \mid i$, then $\mathrm{Tr}_t^n(x_0) = \mathrm{Tr}_t^n(x_0^{2^i})$ and $\mathrm{Tr}_t^n(a) = 0$. To prove the sufficiency, we define the mapping

$$\begin{aligned} \sigma : \ \mathbb{F}_{2^n} &\longrightarrow \mathbb{F}_{2^n} \\ x &\mapsto x^{2^i} + x. \end{aligned}$$

Note that σ is $\mathbb{F}_2$-linear and $\ker(\sigma) = \mathbb{F}_{2^t}$, then $\mathbb{F}_{2^n}/\ker(\sigma) \backsimeq \mathrm{Im}(\sigma)$, and we have then $|\mathrm{Im}(\sigma)| = 2^{n-t}$. Define the set $S = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_t^n(x) = 0\}$, since $\mathrm{Im}(\sigma) \subseteq S$ and $|S| = 2^{n-t}$, then $\mathrm{Im}(\sigma) = S$. This means that the equation $x^{2^i} + x + a = 0$ has a solution in $\mathbb{F}_{2^n}$ for each a satisfying $\mathrm{Tr}_t^n(a) = 0$.

This finishes the proof. □

In what follows, we present a key lemma stating that certain trace values associated with different solutions of a specific affine equation (comprising two linear terms) remain identical.

Lemma 2. *Let* $0 < i < n$ *be a positive integer. Let* $a, b \in \mathbb{F}_{2^n}$, *define*

$$h(x) = \begin{cases} ax + a^{2^i}x^{2^{2i}} + b, & \text{if } v_2(n) > v_2(i), \\ x + x^{2^{2i}} + a, & \text{if } v_2(n) \leq v_2(i). \end{cases}$$

Assume that x_0, y_0 *are two solutions of the equation* $h(x) = 0$, *then we have*

$$\begin{cases} \mathrm{Tr}_1^n(ax_0^{2^i+1}) = \mathrm{Tr}_1^n(ay_0^{2^i+1}), & \text{if } v_2(n) > v_2(i), \\ \mathrm{Tr}_1^n(x_0^{2^i+1} + x_0) = \mathrm{Tr}_1^n(y_0^{2^i+1} + y_0), & \text{if } v_2(n) \leq v_2(i). \end{cases}$$

Proof. The position of $v_2(n)$ with respect to $v_2(i)$ actually induces a precise connection between (n,i) and $(n,2i)$, as expressed by

$$(n,2i) = \begin{cases} 2(n,i), & \text{if } v_2(n) > v_2(i), \\ (n,i), & \text{if } v_2(n) \leq v_2(i). \end{cases} \tag{3.1}$$

Assume $v_2(n) > v_2(i)$. The first observation is that if x_0 satisfies $ax_0 + a^{2^i}x_0^{2^{2i}} = b$, then by multiplying both sides of the equality by $x_0^{2^i}$, we have $ax_0^{2^i+1} + (ax_0^{2^i+1})^{2^i} = bx_0^{2^i}$, which necessarily requires $\mathrm{Tr}_1^n(bx_0^{2^i}) = 0$. Together with

$$\mathrm{Tr}_1^n(a(x_0y_0^{2^i} + x_0^{2^i}y_0)) = \mathrm{Tr}_1^n(x_0^{2^i}(ay_0 + a^{2^i}y_0^{2^{2i}})) = \mathrm{Tr}_1^n(bx_0^{2^i}),$$

we get

$$\begin{aligned} \mathrm{Tr}_1^n(a(x_0^{2^i+1} + y_0^{2^i+1})) &= \mathrm{Tr}_1^n(a(x_0+y_0)^{2^i+1}) + \mathrm{Tr}_1^n(a(x_0y_0^{2^i} + x_0^{2^i}y_0)) \\ &= \mathrm{Tr}_1^n(a(x_0+y_0)^{2^i+1}). \end{aligned}$$

Let $z_0 = x_0 + y_0$, then $az_0 + a^{2^i}z_0^{2^{2i}} = 0$, which implies $az_0^{2^i+1} = a^{2^i}z_0^{2^{2i}+2^i}$, i.e., $az_0^{2^i+1} \in \mathbb{F}_{2^i} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^t}$ with $t = (n,i)$. Hence, we obtain

$$\mathrm{Tr}_1^n(az_0^{2^i+1}) = \mathrm{Tr}_1^t(\mathrm{Tr}_t^n(az_0^{2^i+1})) = \frac{n}{t}\mathrm{Tr}_1^t(az_0^{2^i+1}).$$

The assumption $v_2(n) > v_2(i)$ indicates that $\frac{n}{t}$ is even, then $\mathrm{Tr}_1^n(az_0^{2^i+1}) = 0$ and the result follows.

If $v_2(n) \leq v_2(i)$, then

$$\begin{aligned} & \mathrm{Tr}_1^n(x_0^{2^i+1} + x_0 + y_0^{2^i+1} + y_0) \\ = \ & \mathrm{Tr}_1^n((x_0+y_0)^{2^i+1} + x_0y_0^{2^i} + x_0^{2^i}y_0 + x_0 + y_0) \\ = \ & \mathrm{Tr}_1^n((x_0+y_0)^{2^i+1} + x_0 + y_0) + \mathrm{Tr}_1^n\left(x_0^{2^i}(y_0 + y_0^{2^{2i}})\right) \\ = \ & \mathrm{Tr}_1^n((x_0+y_0)^{2^i+1} + x_0 + y_0) + \mathrm{Tr}_1^n(ax_0^{2^i}). \end{aligned}$$

We have $\mathrm{Tr}_1^n(ax_0^{2^i}) = 0$ due to $ax_0^{2^i} = x_0^{2^i+1} + x_0^{(2^i+1)2^i}$. Thus it suffices to prove that $\mathrm{Tr}_1^n(z_0^{2^i+1} + z_0) = 0$, where $z_0 = x_0 + y_0$ satisfies $z_0^{2^{2i}} + z_0 = 0$. Observe that $z_0 \in \mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{(n,2i)}} = \mathbb{F}_{2^{(n,i)}}$, due to the assumption $v_2(n) \leq v_2(i)$ and $(n,2i) = (n,i)$, we straightforwardly have $z_0^{2^i+1} = z_0^2$ and then we have proven the lemma. □

Remark 1. *Lemma 2 establishes that, whenever the equation $h(x) = 0$ admits multiple solutions, the corresponding trace values — $\mathrm{Tr}_1^n(ax_0^{2^i+1})$ or $\mathrm{Tr}_1^n(x_0^{2^i+1} + x_0)$ depending on*

the conditions in each case — are the same for all roots. Hence, it suffices to choose any single solution x_0 and compute the traces accordingly. In particular, if $v_2(n) > v_2(i)$ and $b = 0$, then for any solution x_0 satisfying $ax_0 + a^{2^i}x_0^{2^{2i}} = 0$, we have $\mathrm{Tr}_1^n(ax_0^{2^i+1}) = 0$, as this equality holds trivially for the zero solution.

To deal with the trace computation concerning (1.2), we need a relation between the two sums $x^{2^t} + x$ and $x^{2^i} + x$, where t is the greatest common divisor of n and i.

Lemma 3. *Let $0 < i < n$ be a positive integer and $t = (n, i)$. Let $a \in \mathbb{F}_{2^n}$ satisfy $\mathrm{Tr}_t^n(a) = 0$. Then, for every $x_0 \in \mathbb{F}_{2^n}$, we have $x_0^{2^i} + x_0 = a$ if and only if $x_0^{2^t} + x_0 = \sum_{j=0}^{\nu-1} a^{2^{ij}}$, where $\nu \in \mathbb{Z}_n$ satisfies $i\nu \equiv t \pmod n$.*

Proof. Note that, by Lemma 1, there exists $x_0 \in \mathbb{F}_{2^n}$ such that $x_0^{2^i} + x_0 = a$.
Such x_0 satisfies:

$$\begin{aligned} x_0^{2^t} &= x_0^{2^{i\nu}} \\ &= (x_0^{2^i})^{2^{i(\nu-1)}} \\ &= (x_0 + a)^{2^{i(\nu-1)}} \\ &= x_0^{2^{i(\nu-1)}} + a^{2^{i(\nu-1)}} \\ &\vdots \\ &= x_0 + \sum_{j=0}^{\nu-1} a^{2^{ij}}, \end{aligned}$$

and the necessity follows. Note that, although the element ν satisfying $i\nu \equiv t \pmod n$ is not unique, the sum $\sum_{j=0}^{\nu-1} a^{2^{ij}}$ is uniquely determined, since if two elements ν_1 and ν_2 satisfy $i\nu_1 \equiv i\nu_2 \equiv t \pmod n$, then we have $\nu_1 \equiv \nu_2 \pmod{\frac{n}{t}}$, and for $\nu_2 = \nu_1 + \frac{n}{t}$, we have:

$$\sum_{j=\nu_1}^{\nu_2-1} a^{2^{ij}} = \sum_{j=0}^{\frac{n}{t}-1} a^{2^{i(j+\nu_1)}} = \Big(\sum_{j=0}^{\frac{n}{t}-1} a^{2^{ij}}\Big)^{2^{i\nu_1}} = \Big(\sum_{j=0}^{\frac{n}{t}-1} a^{2^{tj}}\Big)^{2^{i\nu_1}} = \big(\mathrm{Tr}_t^n(a)\big)^{2^{i\nu_1}} = 0.$$

Indeed, to check the third equality, let us denote by T_1 the ideal of multiples of t in $\mathbb{Z}_n$, that is, $T_1 = \{tj \bmod n : j = 0, 1, \ldots, \frac{n}{t} - 1\}$ and let us denote $T_2 = \{ij \bmod n : j = 0, 1, \ldots, \frac{n}{t} - 1\}$. Then each ij is a multiple of i and then of t, and if two multiples ij_1 and ij_2 are equal, that is, $ij_1 \equiv ij_2 \pmod n$, then $\frac{i}{t}(j_1 - j_2) \equiv 0 \pmod{\frac{n}{t}}$, which means $j_1 \equiv j_2 \pmod{\frac{n}{t}}$. Given the range of j, it follows that the elements $ij \pmod n$ are

distinct for different j. Therefore, the set T_2 consists of exactly all multiples of i modulo n as well.

To prove the sufficiency, we let $b = \sum_{j=0}^{\nu-1} a^{2^{ij}}$. By the assumption $x_0^{2^t} + x_0 = b$, we have

$$\begin{aligned} x_0^{2^i} + x_0 &= b + b^{2^t} + \cdots + b^{2^{t(\frac{i}{t}-1)}} \\ &= b + b^{2^{i\nu}} + \cdots + b^{2^{i\nu(\frac{i}{t}-1)}} \\ &= \sum_{j=0}^{\nu-1} a^{2^{ij}} + \sum_{j=0}^{\nu-1} a^{2^{i(j+\nu)}} + \cdots + \sum_{j=0}^{\nu-1} a^{2^{i(j+(\frac{i}{t}-1)\nu)}} \\ &= \sum_{j=0}^{\frac{i}{t}\nu-1} a^{2^{ij}}. \end{aligned}$$

It suffices for us to prove

$$\sum_{j=0}^{\frac{i}{t}\nu-1} a^{2^{ij}} = a.$$

The set $S = \{ij \bmod n : j = 0, 1, \cdots, \frac{i}{t}\nu - 1\}$ is a subset of T_1, since each element in S is a multiple of t. Moreover, if for some j in $\{0, 1, \ldots, \frac{i}{t}\nu - 1\}$ and j' in $\{0, 1, \ldots, \frac{n}{t} - 1\}$ we have $ij = tj' \pmod n$, then $j\frac{i}{t} = j' \pmod{\frac{n}{t}}$, and j is uniquely determined by j', modulo $\frac{n}{t}$. If $j' = 0$, then the corresponding j can take the values $0, \frac{n}{t}, 2\frac{n}{t}, \ldots, \frac{i}{t}\nu - 1$ (the condition $i\nu \equiv t \pmod n$ implying that $\frac{i}{t}\nu - 1$ is divisible by $\frac{n}{t}$), whose number equals $\frac{\frac{i}{t}\nu-1}{\frac{n}{t}} + 1 = \frac{i\nu-t}{n} + 1$. If $j' \neq 0$, denote j_0 in $[0, 1, \ldots, \frac{n}{t} - 1]$ that is uniquely determined by j', then j takes $\frac{i\nu-t}{n}$ values $j_0, j_0 + \frac{n}{t}, \ldots, j_0 + \frac{i}{t}\nu - 1 - \frac{n}{t}$. Hence, we have

$$\begin{aligned} \sum_{j=0}^{\frac{i}{t}\nu-1} a^{2^{ij}} &= a + \frac{i\nu - t}{n} \sum_{j'=0}^{\frac{n}{t}-1} a^{2^{j't}} \\ &= a + \frac{i\nu - t}{n} \mathrm{Tr}_t^n(a) \\ &= a. \end{aligned}$$

This completes the proof. □

We can now give a complete proof of Theorem 1.

Proof of Theorem 1. The proof proceeds by examining the relationship between the 2-adic orders of n and i.

- If $v_2(n) \leq v_2(i)$, then we have $(n, 2i) = (n, i) = t$ and $\frac{n}{t}$ is odd. Furthermore, since $(2^i + 1, 2^n - 1) = 1$ (because, $2^i - 1$ and $2^i + 1$ being co-prime, we have $(2^i + 1, 2^n - 1) = \frac{(2^{2i}-1, 2^n-1)}{(2^i-1, 2^n-1)} = \frac{2^t-1}{2^t-1} = 1$), the mapping $x \to x^{2^i+1}$ is a permutation of $\mathbb{F}_{2^n}$. Thus (as already stated in Proposition 4), there exists a unique a_1 such that $a = a_1^{2^i+1}$, and we have $a_1 \in \mathbb{F}_{2^t}$ due to the assumption $a \in \mathbb{F}_{2^t}$. Therefore, the equation $H_{i,a,b}(x) = 0$ defined in Proposition 4:

$$x^{2^{2i}} + x + \frac{b}{a_1} + 1 = 0, \tag{3.2}$$

has solutions in $\mathbb{F}_{2^n}$ if and only if (according to Lemma 1) $\mathrm{Tr}^n_{(n,2i)}(\frac{b}{a_1} + 1) = \frac{n}{t}(\frac{b}{a_1} + 1) = 0$, i.e., $b = a_1$. Thus we have $a = a_1^{2^i+1} = b^2$.

  - If $a \neq b^2$, then Equation (3.2) has no solution and $\eta(i, a, b) = 0$.
  - If $a = b^2$, then (3.2) becomes $x^{2^{2i}} + x = 0$. Assume x_0 is a solution, then $x_0 \in \mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{(2i,n)}} = \mathbb{F}_{2^t}$. Therefore, this gives that $\mathrm{Tr}^n_1(x_0^{2^i+1} + x_0) = \frac{n}{t}\mathrm{Tr}^t_1(x_0^2 + x_0) = 0$, i.e., $\eta(i, a, b) = J\left(2, \frac{n'}{(n',i)}\right)^{2^e}$ as shown in Proposition 4.

- If $v_2(n) > v_2(i)$, then $(n, 2i) = 2(n, i) = 2t$ and $\frac{i}{t}$ is odd. By the definition of $G_{i,a,b}(x)$ in Proposition 4, we need to consider the equation

$$x^{2^{2i}} + x = a^{-1}b. \tag{3.3}$$

Observe that $\mathrm{Tr}^n_{(n,2i)}(a^{-1}b) = \frac{n}{2t}a^{-1}b$ due to $a^{-1}b \in \mathbb{F}_{2^t}$, then (3.3) has solutions in $\mathbb{F}_{2^n}$ if and only if either $b = 0$ or $\frac{n}{2t}$ is even.

  - If $v_2(n) = v_2(i) + 1$, i.e., $\frac{n}{2t}$ is odd, we know that (3.3) has no solution for $b \in \mathbb{F}^*_{2^t}$. Hence:
    - If $b \neq 0$, then $\eta_{i,a,b} = 0$ (in other words, $\mathcal{G}(i, a, b) = 0$).
    - If $b = 0$, then obviously any solution x_0 of (3.3) lies in $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{2t}}$. It follows that $x_0^{2^i+1} \in \mathbb{F}_{2^i} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^t}$. Hence $\mathrm{Tr}^n_t(ax_0^{2^i+1}) = 0$, because $\frac{n}{t}$ is even.
  - Assume $v_2(n) > v_2(i) + 1 = v_2(2i)$. In this case, it is obvious that $(n, 4i) = 4t$. Observe that (3.3) is equivalent to the equation system

$$\begin{cases} x^{2^i} + x &= \theta, \\ \theta^{2^i} + \theta &= a^{-1}b. \end{cases}$$

By using Lemma 3, and using that $(a^{-1}b)^{2^{ij}} = a^{-1}b$, we get from the second equation:

$$\theta^{2^t} + \theta = \sum_{j=0}^{\nu_1 - 1} (a^{-1}b)^{2^{ij}} = \nu_1 a^{-1}b, \tag{3.4}$$

where $\nu_1 \in \mathbb{Z}_n$ is such that $i\nu_1 \equiv t \pmod{n}$, which implies that $\theta \in \mathbb{F}_{2^{2t}}$. Assume x_0 is a solution of (3.3). By the first equation in the system, we have

$$\begin{aligned} \mathrm{Tr}_1^n(ax_0^{2^i+1}) &= \mathrm{Tr}_1^n(ax_0^2 + a\theta x_0) \\ &= \mathrm{Tr}_1^n((a^{2^{-1}} + a\theta)x_0) \\ &= \mathrm{Tr}_1^{2t}((a^{2^{-1}} + a\theta)\mathrm{Tr}_{2t}^n(x_0)). \end{aligned}$$

From Lemma 3 and (3.3), we get

$$x_0^{2^{2t}} + x_0 = \sum_{j=0}^{\nu_2 - 1} (a^{-1}b)^{2^{2ij}} = \nu_2 a^{-1}b,$$

where $\nu_2 \in \mathbb{Z}_n$ such that $2i\nu_2 \equiv 2t \pmod{n}$. Therefore,

$$\mathrm{Tr}_{2t}^n(x_0) = x_0 + x_0^{2^{2t}} + \cdots + x_0^{2^{n-2t}} = \frac{n}{4t}\nu_2 a^{-1}b.$$

* If $v_2(n) > v_2(i) + 2$, then $\frac{n}{(n,4i)} = \frac{n}{4t}$ is even, it follows that $\mathrm{Tr}_{2t}^n(x_0) = 0$ and $\mathrm{Tr}_1^n(ax_0^{2^i+1}) = 0$.
* If $v_2(n) = v_2(i) + 2$, then $\frac{n}{4t}$ is odd. Further, since $\frac{n}{2t} \mid \frac{i}{t}\nu_2 - 1$ and $\frac{n}{2t}$ is even, we deduce that ν_2 is odd, too. This gives $\mathrm{Tr}_{2t}^n(x_0) = a^{-1}b$ and then

$$\begin{aligned} \mathrm{Tr}_1^n(ax_0^{2^i+1}) &= \mathrm{Tr}_1^{2t}((a^{2^{-1}} + a\theta)\mathrm{Tr}_{2t}^n(x_0)) \\ &= \mathrm{Tr}_1^{2t}((a^{2^{-1}} + a\theta)a^{-1}b) \\ &= \mathrm{Tr}_1^{2t}(a^{-2^{-1}}b + \theta b) \\ &= \mathrm{Tr}_1^t(b(\theta^{2^t} + \theta)) \\ &= \nu_1 \mathrm{Tr}_1^t(a^{-1}b^2), \end{aligned}$$

  where the third and fourth equalities hold because, under the assumptions that $a, b \in \mathbb{F}_{2^t}$, we have $a^{-2^{-1}}b \in \mathbb{F}_{2^t}$ and consequently $\mathrm{Tr}_1^{2t}(a^{-2^{-1}}b) = \mathrm{Tr}_1^t(\mathrm{Tr}_t^{2t}(a^{-2^{-1}}b)) = 0$. Observe that ν_1 is odd, because $\frac{n}{t}$ is even and $\frac{n}{t} \mid \frac{i}{t}\nu_1 - 1$. Thus, we have $\mathrm{Tr}_1^n(ax_0^{2^i+1}) = \mathrm{Tr}_1^t(a^{-1}b^2)$.

This finishes the proof. □

A straightforward application of Theorem 1 yields the following corollary, which identifies the k-idempotent functions more conveniently among the two classes of Dillon-type bent functions from [34] (see Subsection 2.2).

Corollary 1. *Let n and i be two positive integers and $t = (n, i)$. If $a, b, c \in \mathbb{F}_{2^t}$, $a \neq 0$ and $b \neq c$, then $\mathcal{G}(i, a, b) = \mathcal{G}(i, a, c)$ if and only if one of the following conditions is satisfied:*

(1) $v_2(n) \leq v_2(i)$ *and* $a \notin \{b^2, c^2\}$;

(2) $v_2(n) = v_2(i) + 1$ *and* $bc \neq 0$;

(3) $v_2(n) = v_2(i) + 2$ *and* $\mathrm{Tr}_1^t(a^{-1}(b + c)^2) = 0$;

(4) $v_2(n) > v_2(i) + 2$.

Recall that Propositions 2 and 3 characterize the bentness of $f_{a,1}^d$ ($d \in \mathcal{D}_1$ or $\mathcal{D}_2$) by means of the two equalities $\mathcal{G}(i, a, 1) = \mathcal{G}(i, a, 0)$ and $\mathcal{G}(i-1, a^{2^{-1}}, a^{2^{-i}}) = \mathcal{G}(i-1, a^{2^{-1}}, a^{2^{-i}} + 1)$, respectively. Using Corollary 1, the characterization can be refined by the following proposition.

Proposition 5. *Let n and i be two positive integers.*

1. *For every $a \in \mathbb{F}_{2^t}$ and $d \in \mathcal{D}_1$, denoting $t = (n, i)$, the function $f_{a,1}^d$ is bent if and only if one of the following conditions is satisfied:*

   (1) $v_2(n) \leq v_2(i)$ *and* $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_2 (t \geq 2)$;

   (2) $v_2(n) = v_2(i) + 2$ *and* $\mathrm{Tr}_1^t(a^{-1}) = 0$;

   (3) $v_2(n) > v_2(i) + 2$;

2. *For every $a \in \mathbb{F}_{2^t}$ and $d \in \mathcal{D}_2$, denoting $t = (n, i-1)$, the function $f_{a,1}^d$ is bent if and only if one of the following conditions is satisfied:*

   (1) $v_2(n) \leq v_2(i-1)$ *and* $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^2}$ *(where $t \geq 3$)*;

   (2) $v_2(n) = v_2(i-1) + 1$ *and* $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_2$ *(where $t \geq 2$)*;

   (3) $v_2(n) = v_2(i-1) + 2$ *and* $\mathrm{Tr}_1^t(a^{-1}) = 0$;

   (4) $v_2(n) > v_2(i-1) + 2$.

Proof. The proof straightforwardly follows from Corollary 1 and we only illustrate case 2. The four conditions are derived by noting that for $t = (n, i-1)$ and $a \in \mathbb{F}_{2^t}$, the assumption $a^{2^{-i}} = a^{2^{n-(i-1)-1}} = a^{2^{-1}}$ leads to two subcases: $a^{2^{-1}} = (a^{2^{-i}})^2$ simplifies to $a = 1$, while $a^{2^{-1}} = (a^{2^{-i}})^2 + 1$ means $a^2 + a + 1 = 0$, restricting $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Therefore, $a^{2^{-1}} \notin \{(a^{2^{-i}})^2, (a^{2^{-i}})^2 + 1\}$ holds precisely when $a \notin \mathbb{F}_{2^2}$, which yields Condition (1). If $v_2(n) = v_2(i-1) + 1$, obviously it suffices to have $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_2$, which is exactly Condition (2). Condition (3) arises from $\mathrm{Tr}_1^t(a^{-2^{-1}}) = \mathrm{Tr}_1^t(a^{-1}) = 0$, and Condition (4) is direct. □

3.2 On the k-idempotent property of $f_{a,1}^d$ with $d \in \mathcal{D}$

By Proposition 1 in the Preliminary section, establishing the k-idempotent property for a family of Boolean functions requires verifying two conditions:

- All coefficients must be constrained to the subfield $\mathbb{F}_{2^k}$;
- For every proper divisor l of k, there exists at least one coefficient a_i that does not belong to $\mathbb{F}_{2^l}$.

Equivalently, we investigate whether functions generated with coefficients from $\mathbb{F}_{2^k}$ – with at least one coefficient not belonging to any proper subfield $\mathbb{F}_{2^l}$ – maintain their membership within the original family.

Recall that for $d \in \mathcal{D}$, the function $f_{a,1}^d$ of Relation (1.1) is determined by the coefficient a, thus from Proposition 5, it is convenient for us to identify these integers i, such that $f_{a,1}^d$ is k-idempotent bent for a divisor k of n. Denoting

$$C(k) = \{\alpha \in \mathbb{F}_{2^n} : deg(m_\alpha(x)) = k\}, \tag{3.5}$$

where $m_\alpha(x) \in \mathbb{F}_2[x]$ is the minimal polynomial of α (i.e., the monic irreducible polynomial of the smallest degree such that $m_\alpha(\alpha) = 0$). It is obvious for a fixed k and $a \in C(k)$ that a does not belong to any subfield smaller than $\mathbb{F}_{2^k}$ and the k-idempotent bentness of $f_{a,1}^d$ ($d \in \mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$) is characterized in the following proposition.

Proposition 6. *Let n, i and k be three positive integers.*

1. *If $d \in \mathcal{D}_1$, $t = (n, i)$ and $k \mid t$, then for $a \in C(k)$, where $C(k)$ is defined in (3.5), the function $f_{a,1}^d$ is k-idempotent bent if and only if one of the following three conditions is satisfied:*

(1) $v_2(n) \leq v_2(i)$ *and* $k \geq 2$;

(2) $v_2(n) = v_2(i) + 2$, *either* $\mathrm{Tr}_1^k(a^{-1}) = 0$ *or* ($\mathrm{Tr}_1^k(a^{-1}) = 1$ *and* $\frac{t}{k}$ *is even);*

(3) $v_2(n) > v_2(i) + 2$;

2. *If* $d \in \mathcal{D}_2$, $t = (n, i-1)$ *and* $k \mid t$, *then for* $a \in C(k)$, *the function* $f_{a,1}^d$ *is* k*-idempotent bent if and only if one of the following four conditions is satisfied:*

(1) $v_2(n) \leq v_2(i-1)$ *and* $k \geq 3$;

(2) $v_2(n) = v_2(i-1) + 1$ *and* $k \geq 2$;

(3) $v_2(n) = v_2(i-1) + 2$, *either* $\mathrm{Tr}_1^k(a^{-1}) = 0$ *or* ($\mathrm{Tr}_1^k(a^{-1}) = 1$ *with* $\frac{t}{k}$ *even);*

(4) $v_2(n) > v_2(i-1) + 2$.

Proof. The proof follows directly from Proposition 5, it suffices for us to illustrate the case $d \in \mathcal{D}_1$ as an example. Recall that $f_{a,1}^d$ is bent if and only if $\mathcal{G}(i, a, 0) = \mathcal{G}(i, a, 1)$. Then the characterization of the k-idempotent bentness of $f_{a,1}^d$, i.e.,, $a \in C(k) \subset \mathbb{F}_{2^t}$, is equivalent to satisfying one of the three conditions. When $v_2(n) \leq v_2(i)$, the condition $a \notin \mathbb{F}_2$ in Proposition 5 is equivalent to $k \geq 2$ (since $a \in C(k) \subset \mathbb{F}_{2^t} \setminus \mathbb{F}_2$). For the case $v_2(n) = v_2(i) + 2$, since $\mathrm{Tr}_1^t(a^{-1}) = \frac{t}{k}\mathrm{Tr}_1^k(a^{-1})$, the condition $\mathrm{Tr}_1^t(a^{-1}) = 0$ holds if and only if either $\mathrm{Tr}_1^k(a^{-1}) = 0$, or $\mathrm{Tr}_1^k(a^{-1}) = 1$ and $\frac{t}{k}$ is even. When $v_2(n) > v_2(i) + 2$, the above condition is direct from Condition (3) in Proposition 5. □

Based on the preceding analysis, for any prescribed integer k and an initially selected $a \in C(k)$, the k-idempotent bentness reduces to characterizing the integers n and i via the 2-adic orders. This naturally leads to a question: Given a positive integer n, does there exist a Boolean function in partial spread class that is k-idempotent bent for every divisor k of n? In what follows, we provide an affirmative answer to this question for the case $k \geq 3$. Recall that a polynomial is called *irreducible* if it cannot be factored into lower-degree non-constant polynomials [18].

First introduced by Möbius [27] and formally defined by Mertens [22], the Möbius function is an important arithmetic function in number theory, which depends on the factorizations of integers. It is defined by $\mu : \mathbb{N} \to \{-1, 0, 1\}$ as [18]:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is square-free with } k \text{ distinct prime factors}, \\ 0 & \text{if } n \text{ has a squared prime factor.} \end{cases}$$

Although computing the Möbius function is computationally demanding (due to its dependence on integer factorization), the function itself is of critical importance, especially as a combinatorial tool to invert certain number-theoretic relations. Notably, a counting formula for the number of irreducible polynomials over $\mathbb{F}_q$ involving the Möbius function is given as follows [18]:

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, q^d, \tag{3.6}$$

where $N_q(n)$ denotes the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. Using equation (3.6), we have the following lemma:

Lemma 4. *Let $k \geq 3$ and $k \,|\, n$ be a positive integer. Then there exists an element $\alpha \in C(k)$ satisfying $\mathrm{Tr}_1^k(\alpha) = 0$.*

Proof. Denote by $I(k)$ the cardinality of the set $C(k)$, then it follows that $I(k) = kN_2(k)$, where $N_2(k)$ is defined as in Proposition 3.6 for the case $q = 2$. Thus we have

$$\begin{aligned} I(k) &= \sum_{s|k} \mu\left(\frac{k}{s}\right) 2^s \\ &> 2^k - \sum_{s|k, s\neq k} 2^s \\ &> 2^k - \sum_{s=0}^{\lceil \frac{k}{2} \rceil} 2^s \\ &= 2^k - (2^{\lceil \frac{k}{2} \rceil + 1} - 1) \\ &= 2^{k-1} + 2^{k-1} - 2^{\lceil \frac{k}{2} \rceil + 1} + 1 \\ &> 2^{k-1}, \end{aligned}$$

if $k - 1 \geq \lceil \frac{k}{2} \rceil + 1$, i.e., $k \geq 4$. Since the number of elements $\alpha \in \mathbb{F}_{2^k}$ with $\mathrm{Tr}_1^k(\alpha) = 1$ exactly equals 2^{k-1}, there exists some $\alpha \in C(k)$ such that $\mathrm{Tr}_1^k(\alpha) = 0$. The case $k = 3$ is easy to verified.

This completes the proof. □

Based on Lemma 4, we can always select a coefficient $a \in C(k)$ with $\mathrm{Tr}_1^k(a^{-1}) = 0$ for $k \geq 3$. For such a, the last two conditions in Proposition 6 can be unified as either $v_2(n) \geq v_2(i) + 2$, or $v_2(n) \geq v_2(i-1) + 2$, depending on the respective cases.

Theorem 2. *Let n be a positive integer. For each divisor k of n with $k \geq 3$, select integers i such that:*

- $k \mid i-1$ *(*$i = k+1$ *for example),*
- $a \in C(k)$ *satisfies* $\mathrm{Tr}_1^k(a^{-1}) = 0$*,*

then the corresponding $f_{a,1}^d$ *is* k*-idempotent bent for* $d \in \mathcal{D}_2$*.*

Proof. Note that $a \in C(k)$ with $k \geq 3$, then by the selection of i, the three conditions on the k-idempotent bentness of $f_{a,1}^d$ for $d \in \mathcal{D}_2$ are:

- $v_2(n) \leq v_2(i-1)$ and $a \notin \mathbb{F}_{2^2}$;
- $v_2(n) = v_2(i-1) + 1$ and $a \notin \mathbb{F}_2$;
- $v_2(n) \geq v_2(i-1) + 2$.

Thus precisely one of the three conditions is satisfied for each i.

This proves the theorem. □

However, for $k = 1, 2$, the same conclusion can not be established because a is restricted to either 1 or $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Consequently, characterizing the k-idempotent bentness of $f_{a,1}^d$ completely reduces to the selection of integer pairs n and i, and we summarizing the the conditions in Propositions 7 and 8. (Both the proofs are straightforward and thus omitted.)

Proposition 7. *Let* n *and* i *be two positive integers.*

1. *Let* $d \in \mathcal{D}_1$*, then* $f_{1,1}^d$ *is* 1*-idempotent bent if and only if* n *and* i *satisfy one of the following conditions:*
   - $v_2(n) = v_2(i) + 2$ *and* i *is even;*
   - $v_2(n) > v_2(i) + 2$*;*
2. *Let* $d \in \mathcal{D}_2$*, then* $f_{1,1}^d$ *is* 1*-idempotent bent if and only if one of the following conditions is satisfied:*
   - $v_2(n) = v_2(i-1) + 2$ *and* i *is odd;*
   - $v_2(n) > v_2(i-1) + 2$.

Example 1. *From Proposition 7, it is necessary that* $8 \mid n$*. Let* $n = 8$*, we partition the sets* $\mathcal{D}_1$ *and* $\mathcal{D}_2$ *according to the conditions:*

- *Partitions of* $\mathcal{D}_1$*:*
  - $\mathcal{D}_{11} = \{31869, 24159\}$ *for* $i = 2, 6$
  - $\mathcal{D}_{12} = \{32126, 31355, 28271, 15935\}$ *for* $i = 1, 3, 5, 7$
- *Partitions of* $\mathcal{D}_2$*:*
  - $\mathcal{D}_{21} = \{63739, 48319\}$ *for* $i = 3, 7$
  - $\mathcal{D}_{22} = \{64253, 62711, 56543\}$ *for* $i = 2, 4, 6$

Thus, the function $f_{1,1}^d$ *on* $\mathbb{F}_{2^{16}}$ *is* 1*-idempotent for* $d \in \mathcal{D}_1 \cup \mathcal{D}_2$*, where* $\mathcal{D}_1 = \mathcal{D}_{11} \cup \mathcal{D}_{12}$ *and* $\mathcal{D}_2 = \mathcal{D}_{21} \cup \mathcal{D}_{22}$*.*

Proposition 8. *Let* n *and* i *be two positive integers and* $a \in \mathbb{F}_{2^n}$ *satisfy* $a^2 + a + 1 = 0$*. We have*

1. *Let* $d \in \mathcal{D}_1$ *and* $2 \,|\, (n, i)$*, then* $f_{a,1}^d$ *is* 2*-idempotent bent if and only if* n *and* i *satisfy one of the following conditions:*
   - $v_2(n) \leq v_2(i)$*;*
   - $v_2(n) = v_2(i) + 2$ *and* $v_2(i) \geq 2$*;*
   - $v_2(n) > v_2(i) + 2$*;*
2. *Let* $d \in \mathcal{D}_2$ *and* $2 \,|\, (n, i-1)$*, then* $f_{a,1}^d$ *is* 2*-idempotent bent if and only if* n *and* i *satisfy one of the following conditions:*
   - $v_2(n) = v_2(i-1) + 1$*;*
   - $v_2(n) = v_2(i-1) + 2$ *and* $v_2(i-1) \geq 2$*;*
   - $v_2(n) > v_2(i-1) + 2$*.*

Example 2. *Let* $n = 12$*. For each type of* d*, exactly one condition can be satisfied, which yields:*

- $\mathcal{D}_1 = \{8349687, 7858047\}$ *for* $i = 4, 8$
- $\mathcal{D}_2 = \{16748539, 16502719, 12569599\}$ *for* $i = 3, 7, 11$

Consequently, the function $f_{a,1}^d$ *on* $\mathbb{F}_{2^{24}}$ *is* 2*-idempotent for* $d \in \mathcal{D}_1 \cup \mathcal{D}_2$*.*

4 Conclusion

In this paper, we studied the existence and constructions of k-idempotent bent functions in the partial spread class. Our main results established the existence of such functions for each divisor $k \geq 3$ of n. For the cases $k = 1, 2$, explicit conditions on n and i were described. The core problem reduced to solving a special linear equation and computing the associated trace function. The reformulation of the target equation as a system of two linear equations enabled explicit computation through the transitivity property of trace maps. To our knowledge, this is the first time that k-idempotent functions in $\mathcal{PS}$ class are identified. However, it should be noted that, our results rely heavily on the computation of $\eta_{i,a,b}$ in Theorem 1, which imposes strong restrictions on the coefficients a and b (requiring both a and b in $\mathbb{F}_{2^{(n,i)}}$). It is worth further investigating the removal of the restrictions and the implications for analyzing the k-idempotent bent property of functions.

Acknowledgement

The work of X. Zeng was supported by the National Key Research and Development Program of China (No. 2021YFA1000600). The work of Z. Tu and X. Zeng was supported by the National Natural Science Foundation of China under Grants 12271145, 12471492, and the Natural Science Foundation of Hubei Province of China under Grant 2023AFB841, and by the Innovation Group Project of the Natural Science Foundation of Hubei Province of China under Grant 2023AFA021.

References

[1] C.M. Adams, Constructing symmetric ciphers using the CAST design procedure. Des. Codes Cryptogr. 12(3), pp. 283–316, 1997.

[2] E.R. Berlekamp, L.R. Welch, Weight distributions of the cosets of the (32, 6) Reed-Muller code. IEEE Trans. Inf. Theory 18(1), pp. 203–207, 1972.

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

[4] C. Carlet, G. Gao, W. Liu, A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. J. Comb. Theory, Ser. A, 127, pp. 161–175, 2014.

[5] L. Carlitz, Explicit evaluation of certain exponential sums. Mathematica Scandinavica 44(1), pp. 5–16, 1979.

[6] A. Canteaut, P. Charpin, G. Kyureghyan, A new class of monomial bent functions. Finite Fields Appl. 14(1), pp. 221–241, 2008.

[7] P. Charpin, G. Kyureghyan, Cubic monomial bent functions: A subclass of $\mathcal{M}$. SIAM J. Discrete Math. 22(2), pp. 650–665, 2008.

[8] J. Dillon, Elementary Hadamard difference sets. PhD dissertation, University of Maryland, 1974.

[9] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, P. Gaborit, Construction of bent functions via Niho power functions. J. Combin. Theory Ser. A, 113(5), pp. 779–798, 2006.

[10] E. Filiol, C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation immunity. In: Proceedings of EUROCRYPT-98. LNCS 1403, pp. 475–488, 1998.

[11] C. Fontaine, On some cosets of the first-order Reed-Muller code with high minimum weight. IEEE Trans. Inf. Theory 45(4), pp. 1237–1243, 1999.

[12] X. Hou, Explicit evaluation of certain exponential sums of binary quadratic functions. Finite Fields Appl. 13(4), pp. 843–868, 2007.

[13] S. Kavut, M.D. Yücel, Generalized rotation symmetric and dihedral symmetric Boolean functions-9 variable Boolean functions with nonlinearity 242. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 2007, LNCS 485, pp. 321–329, 2007. Springer, Berlin.

[14] G. Leander, Monomial bent functions. IEEE Trans. Inf. Theory 52(2), pp. 738–743, 2006.

[15] G. Leander, A. Kholosha, Bent functions with 2^r Niho exponents. IEEE Trans. Inf. Theory 52(12), pp. 5529–5532, 2006.

[16] N. Li, T. Helleseth, X. Tang, A. Kholosha, Several new classes of bent functions from Dillon exponents. IEEE Trans. Inf. Theory 59(3), pp. 1818–1831, 2013.

[17] Y. Li, H. Kan, S. Mesnager, J. Peng, C.H. Tan, L. Zheng, Generic constructions of (Boolean and vectorial) bent functions and their consequences. IEEE Trans. Inf. Theory 68(4), pp. 2735–2751, 2022.

[18] R. Lidl, H. Niederreiter, Finite Fields. Encyclopedia Math. Appl. Cambridge University Press, 1997.

[19] P. Lisonek, M.J. Moisio, On zeros of Kloosterman sums. Des. Codes Cryptogr. 59(1-3), pp. 223–230, 2011.

[20] W. Ma, M. Lee, and F. Zhang. A new class of bent functions. IEICE Trans. Fundamentals, E88-A(7), pp. 2039–2040, 2005.

[21] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland. 1977.

[22] F. Mertens, Über einige asymptotische Gesetze der Zahlentheorie. J. reine angew. Math. 77, pp. 46–62, 1874.

[23] S. Mesnager, Bent Functions: Fundamentals and Results. Springer Cham, Switzerland, 2016.

[24] S. Mesnager, A new class of bent and hyper-bent Boolean functions in polynomial forms. Des. Codes Cryptogr. 59(1-3), pp. 265–279, 2011.

[25] S. Mesnager, Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory 57(9), pp. 5996–6009, 2011.

[26] S. Mesnager. Chapter "Linear codes from functions" Concise encyclopedia of coding theory, CRC Press (W.C. Huffman, J.L. Kim, P. Solé Eds.), 2021.

[27] A.F. Möbius, Über eine besondere Art von Umkehrung der Reihen. J. reine angew. Math. 9, pp. 105–123, 1832.

[28] J.J. Mykkeltveit, The covering radius of the (128, 8) Reed-Muller code is 56. IEEE Trans. Inf. Theory 26(3), pp. 359–362, 1980.

[29] N.J. Patterson, D.H. Wiedemann, The covering radius of the (215, 16) Reed-Muller code is at least 16276. IEEE Trans. Inf. Theory 29(3), pp. 354–356, 1983, see also the correction in IEEE Trans. Inf. Theory 36(2), pp. 443, 1990.

[30] J. Pieprzyk, C. Qu, Fast hashing and rotation symmetric functions. J. Univ. Comput. Sci. 5(1), pp. 20–31, 1999.

[31] O.S. Rothaus, On bent functions. J. Combin. Theory Ser. A, 20(3), pp. 300–305, 1976.

[32] S. Su, X. Tang, Systematic constructions of rotation symmetric bent functions, 2-rotation symmetric bent functions, and bent idempotent functions. IEEE Trans. Inf. Theory 63(7), pp. 4658–4667, 2017.

[33] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, T. Helleseth, Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Trans. Inf. Theory 63(10), pp. 6149–6157, 2017.

[34] Z. Tu, C. Li, X. Zeng, T. Helleseth, N. Li, New characterizations of Dillon-like hyperbent functions via Dickson polynomials. J. Cryptol. 38(4), article number 35, 2025.

[35] N.Y. Yu, G. Gong, Constructions of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory 52(7), pp. 3291–3299, 2006.