PAPER

Numerical Results and Asymptotic Lower Bound on the Covering Radius of Reed-Muller Codes RM(2, 11) and RM(3, n)

Jinjie GAO†a), ***Member***

SUMMARY The covering radius of the r-th order Reed-Muller code RM(r, n), denoted by $\rho(r, n)$, is the maximum r-th order nonlinearity of n-variable Boolean functions. Using the Fourquet-Tavernier list-decoding algorithm and the Fourquet list-decoding algorithm, we discover, among monomial Boolean functions, 11-variable Boolean functions with second-order nonlinearity 856, and we determine that the covering radius of RM(3, 8) in RM(4, 8) is 56. Besides, it is proved that the complexity of the Fourquet algorithm for list decoding RM(r, n) is linear in the length of the code 2^n given the decoding radius up to the Johnson bound. In this paper, we prove that the complexity of the Fourquet algorithm is also linear in 2^n in some special cases when the decoding radius is close to 2^{n-r}. Moreover, following from the Carlet's method, we improve the best proven lower bound on the third-order nonlinearity of monomial Boolean functions. In a word, the original idea of our work is to improve the lower bound on $\rho(r, n)$ according to two categories as follows: for small r and n, we search an n-variable Boolean function with larger r-th order nonlinearity using a list-decoding algorithm for Reed-Muller codes; for large n, we study a class of quartic monomial Boolean functions to improve the best proven lower bound on its third-order nonlinearity.

key words: *covering radius, Reed-Muller codes, high-order nonlinearity, monomial Boolean functions, list decoding*

1. Introduction

Determining the covering radius of the Reed-Muller codes is a difficult task, even for small dimensions. The r-th order Reed-Muller code, denoted by RM(r,n), consists of all n-variable Boolean functions of degree at most r. The *covering radius* of a code is the smallest integer ρ such that any vector in the vector space is within Hamming distance ρ from some codeword. The covering radius of Reed-Muller codes RM(r,n) is denoted by $\rho(r,n)$. By definition, $\rho(r,n)$ is also the maximum r-th order nonlinearity for n-variable Boolean functions.

For some small r and n, to *lower bound* $\rho(r,n)$, it is sufficient to exhibit a Boolean function with large r-th order nonlinearity. The categories of methods to lower bound $\rho(r,n)$ include constructing an Boolean function with large (high-order) nonlinearity by its algebraic normal form or by concatenation, searching Boolean functions with large (high-order) nonlinearity using heuristic search algorithm or list-decoding algorithm for Reed-Muller codes, and classifying all non-equivalent cosets in the quotient space of RM(k,n)/RM(r,n).

For first-order nonlinearity, Berlekamp and Welch [1] classified all cosets of RM(1,5) into 48 non-equivalent classes by hand and proved $\rho(1,5) = 12$. Patterson and Wiedemann [23] studied a class of Boolean functions on $3 \times 5 = 15$ variables, which is invariant under the action of the cyclic group $\mathbb{F}^*_{2^3} \cdot \mathbb{F}^*_{2^5}$ as well as the Frobenius automorphism $x \mapsto x^2$ for $x \in \mathbb{F}_2^{15}$. They found two cosets of RM(1, 15) with first-order nonlinearity 16276 of this type by determining their weight distributions by hand, which implies that $\rho(1,15) \geq 16276$. By concatenating a Patterson-Wiedemann function on 15 variables and a bent function, one can construct an n-variable Boolean function with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$ for any odd $n > 15$. Using steepest descent like iterative heuristic search algorithm, Kavut and Yücel [17] found 9-variable Boolean functions with first-order nonlinearity 242 in the *generalized rotation symmetric class* and thus proved that $\rho(1,9) \geq 242$. By concatenating a bent function in 2 or 4 variables and the above-mentioned 9-variable function, they showed that $\rho(1,11) \geq 996$ and $\rho(1,13) \geq 4040$. Using a heuristic search algorithm, Kavut and Maitra [18] found a Patterson-Wiedemann type function on 21 variables with first-order nonlinearity $2^{21-1} - 2^{\frac{21-1}{2}} + 16$.

For the second-order nonlinearity, Schatz [24] constructed a cubic 6-variable Boolean function with second-order nonlinearity 18 by concatenating a 5-variable Boolean function with nonlinearity 12 and a 5-variable Boolean function with second-order nonlinearity 6. Thus, Schatz proved that $\rho(2,6) \geq 18$. Wang [26] proved that $\rho(2,7) = 40$. Hou [15] gave a complete classification of all non-equivalent cosets of RM(2, 8) in RM(3, 8), among which the largest second-order nonlinearity is 88, and thus proved that $\rho(2,8) \geq 88$. By the classification of the quotient space of RM(3,9)/RM(2,9), Brier and Langevin [2] proved that the covering radius of RM(2,9) in RM(3,9) is 196. Fourquet and Tavernier [9] proposed a list decoding algorithm for decoding the second-order Reed-Muller code RM($2,n$) for any distance. Using that decoding algorithm, they discovered a 9-variable monomial Boolean function $\mathrm{tr}_9(x^{73})$ with second-order nonlinearity 196, a 10-variable monomial Boolean function $\mathrm{tr}_{10}(x^{35})$ with second-order nonlinearity 400, two 11-variable monomial Boolean functions with second-order nonlinearity 848 and a 12-variable monomial Boolean function with second-order nonlinearity 1760. Therefore, $\rho(2,9) \geq 196$, $\rho(2,10) \geq 400$, $\rho(2,11) \geq 848$ and $\rho(2,12) \geq 1760$. Fourquet [10] generalized the above algorithm for high-order Reed-Muller codes; the complexity

Manuscript received January 25, 2025.
Manuscript revised April 21, 2025.
Manuscript publicized July 18, 2025.
†School of Data Science and Engineering, East China Normal University, Shanghai 200062, China.
a) E-mail: jjgao@dase.ecnu.edu.cn
DOI: 10.1587/transfun.2025EAP1015

of the Fourquet algorithm is linear in the length of the code 2^n when the decoding distance is within the Johnson bound.

For the third-order nonlinearity, Gao et al. [11] classified all 7-variable Boolean functions into 66 types and proved that there exists no one 7-variable Boolean function with third-order nonlinearity exceeding 20 using an exhaustive search, that is, $\rho(3,7) = 20$. Independently, Gillot and Langevin [13] gave another proof of $\rho(3,7) = 20$ by giving a classification of the quotient space of $\mathrm{RM}(7,7)/\mathrm{RM}(3,7)$. Langevin and Leander [20] classified all non-equivalent cosets of $\mathrm{RM}(4,8)/\mathrm{RM}(3,8)$, among which there is a coset with third-order nonlinearity ≥ 50, which implies that $\rho(3,8) \geq 50$.

For higher-order nonlinearities, Gillot and Langevin [14] proved that $\rho(4,8) = 26$ using a classification algorithm. Dougherty, Mauldin and Tiefenbruck [8] provided a method for proving the lower bound on the distance from a function $f \in \mathrm{RM}(n-3,n)$ to any codeword in $\mathrm{RM}(n-4,n)$. By applying these methods, they proved that the covering radius of $\mathrm{RM}(5,9)$ in $\mathrm{RM}(6,9)$ is between 28 and 32. Their method heavily depends on the classification of $\mathrm{RM}(3,n)/\mathrm{RM}(2,n)$. Notice that almost all concrete results we mention above need the assistance of computers, except for the proof of $\rho(1,5) = 12$ and $\rho(1,15) \geq 16276$.

For most small r and n, we observe that n-variable functions with large r-th order nonlinearity can be found among monomial Boolean functions according to the previous works. For large n, searching for Boolean functions with large high-order nonlinearities, we believe that monomial Boolean functions are good candidates to study both theoretically [12] and experimentally.

1.1 Our Result

In our work, we implement the Fourquet-Tavernier algorithm [9] and the Fourquet algorithm [10] to compute the r-th order nonlinearity of a Boolean function with a few improvements. We discover some 11-variable monomial Boolean functions with second-order nonlinearity 856 and we determine the largest third-order nonlinearity among all the non-equivalent cosets in the quotient space $\mathrm{RM}(4,8)/\mathrm{RM}(3,8)$ is 56. So we prove the following theorems.

Theorem 1. $\rho(2,11) \geq 856$.

Theorem 2. *The covering radius of* $\mathrm{RM}(3,8)$ *in* $\mathrm{RM}(4,8)$ *is 56.*

Given the decoding radius up to the Johnson bound, it is proved that the Fourquet list-decoding algorithm has linear complexity in the length of code [10]. In this paper, we prove that the complexity of the Fourquet algorithm is linear in 2^n in some special cases given the decoding radius close to 2^{n-r} instead of the Johnson bound.

Theorem 3. *Given the decoding radius of* $2^{n-r} - \epsilon$ *for* $\epsilon > 0$ *and* $r \ll n$*, there exists an n-variable Boolean function f such that the Fourquet list-decoding algorithm outputs all codewords in* $\mathrm{RM}(r,n)$ *within distance* $2^{n-r} - \epsilon$ *from f with linear complexity in* 2^n.

Furthermore, inspired by the work in [12], we improve the best proven lower bound on the third-order nonlinearity of monomial Boolean functions.

Theorem 4. *Let* $f = \mathrm{tr}_n(x^{15})$. *For even* $n \geq 6$*, we have*

$$\begin{aligned} &\mathrm{nl}_3(f) \geq 2^{n-1} - \\ &\frac{1}{2}\sqrt{(2^n-1)\sqrt{\frac{7}{3}\cdot 2^{\frac{3}{2}n+1} + 5\cdot 2^{n+1} - \frac{1}{3}\cdot 2^{\frac{n}{2}+5}} + 2^n} \\ &= \ 2^{n-1} - 2^{\frac{7n}{8}-\frac{3}{4}+\frac{1}{4}\log_2\frac{7}{3}} - O(2^{\frac{3}{8}n}) \end{aligned}$$

for $3 \nmid n$.

$$\begin{aligned} &\mathrm{nl}_3(f) \geq 2^{n-1} - \\ &\frac{1}{2}\sqrt{(2^n-1)\sqrt{\frac{7}{3}\cdot 2^{\frac{3}{2}n+1} + 7\cdot 2^{n+1} - \frac{1}{3}\cdot 2^{\frac{n}{2}+5}} + 2^n} \\ &= \ 2^{n-1} - 2^{\frac{7n}{8}-\frac{3}{4}+\frac{1}{4}\log_2\frac{7}{3}} - O(2^{\frac{3}{8}n}) \end{aligned}$$

for $3 \mid n$.

For odd n, we have

$$\begin{aligned} &\mathrm{nl}_3(f) \geq 2^{n-1} - \\ &\frac{1}{2}\sqrt{(2^n-1)\sqrt{3\cdot 2^{\frac{3n+1}{2}} + (5\cdot 2^{\frac{3}{2}}+2)2^n - 2^{\frac{n+7}{2}}} + 2^n} \\ &= \ 2^{n-1} - 2^{\frac{7n}{8}-\frac{7}{8}+\frac{1}{4}\log_2 3} - O(2^{\frac{3}{8}n}) \end{aligned}$$

for $3 \nmid n$.

$$\begin{aligned} &\mathrm{nl}_3(f) \geq 2^{n-1} - \\ &\frac{1}{2}\sqrt{(2^n-1)\sqrt{3\cdot 2^{\frac{3n+1}{2}} + (2^{\frac{9}{2}}+2)2^n - 2^{\frac{n+7}{2}}} + 2^n} \\ &= \ 2^{n-1} - 2^{\frac{7n}{8}-\frac{7}{8}+\frac{1}{4}\log_2 3} - O(2^{\frac{3}{8}n}) \end{aligned}$$

for $3 \mid n$.

Previous to our results, it was known that $\rho(2,11) \geq 848$ [9] and $\rho(3,8) \geq 50$ [20]. For more backgrounds and results on $\rho(r,n)$, we send interested readers to [7]. We give an updated table on $\rho(r,n)$ for $n \leq 11$ in Table 1. (Note that $\rho(n-3,n) = \begin{cases} n+2, & \text{for even } n \\ n+1, & \text{for odd } n \end{cases}$, which was proved by McLoughlin [21].)

2. Preliminary

Let $\mathbb{F}_2$ be the finite field of size 2. Any n-variable Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be written as a unique multilinear polynomial in $\mathbb{F}_2[x_1, x_2 \ldots, x_n]$, that is,

$$f(x_1, x_2, \ldots, x_n) = \sum_{S\subseteq[n]} c_S \prod_{i\in S} x_i,$$

which is called the *algebraic normal form* (ANF). The *algebraic degree* of f, denoted by $\deg(f)$, is the maximum

Table 1 Bounds on $\rho(r,n)$ for $n \le 11$.

r \ n	3	4	5	6	7	8
1	2	6	12[1]	28	56[22]	120
2	1	2	6	18[24]	40[26]	88[15]-96
3	0	1	2	8	20[11]	**56**[Theorem 2]-60
4		0	1	2	8	26[14]
5			0	1	2	10
6				0	1	2
7					0	1
8						0

r \ n	9	10	11
1	242[17]-244	496	996[17]
2	196[2]-216	400[9]-460	**856**[Theorem 1]-956
3	111-156	**194**[Table 11]-372	**454**[Table 10]-832
4	58-86	≤ 242	≤ 614
5	28[8] – 36	≤ 122	≤ 364
6	10	≤ 46	≤ 168
7	2	12	≤ 58
8	1	2	12
9	0	1	2
10		0	1
11			0

$\rho(1,1) = 0$.
$\rho(1,2) = 1, \rho(2,2) = 0$.
$\rho(r,n) \le \rho(r-1,n-1) + \rho(r,n-1)$ [24].

size of S with $c_S \neq 0$ in its ANF. We denote the set of all n-variable Boolean functions by $\mathcal{B}_n$.

The *Hamming weight* of a Boolean function f, denoted by $\mathrm{wt}(f)$, is the cardinality of the set $\{x \in \mathbb{F}_2^n : f(x) = 1\}$. The *distance* between two functions f and g is the cardinality of the set $\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}$, denoted by $\mathrm{d}(f,g)$.

Lemma 1. *[16, Lemma 2.2] Let $1 \le r \le n$, and $s \le r$. For any $f \in \mathrm{RM}(r,n)$, $g \in \mathrm{RM}(s,n)$, we have*

$$\mathrm{wt}(f+g) \equiv \mathrm{wt}(f) \pmod{2^{\lceil \frac{n-s}{r} \rceil}}.$$

For $1 \le r \le n$, the *r-th order nonlinearity* of an n-variable Boolean function f, denoted by $\mathrm{nl}_r(f)$, is the minimum distance between f and Boolean functions with degree at most r, i.e.,

$$\mathrm{nl}_r(f) = \min_{\deg(g) \le r} \mathrm{d}(f,g).$$

We denote by $\mathrm{nl}(f)$ the *first-order nonlinearity* of f.

The *general linear group* over $\mathbb{F}_2$, denoted by $\mathrm{GL}(n) = \mathrm{GL}(n,\mathbb{F}_2)$, is the set of all $n \times n$ invertible matrices with the operation of matrix multiplication. An *affine transformation* $L : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ is defined as $L(x) = Ax+b$ for some $A \in \mathrm{GL}(n)$ and $b \in \mathbb{F}_2^n$. We denote the action of the affine transformation L on f by $f \circ L = f(L(x))$. Denote by $\mathrm{AGL}(n)$ the group consisting of all affine transformations.

Let $f, g \in \mathcal{B}_n$. The Boolean function f is *affine equivalent* to g if there exists $L \in \mathrm{AGL}(n)$ such that $f \circ L = g$. We denote by $\mathrm{RM}(r,n)/\mathrm{RM}(s,n)$ the quotient space consisting of all cosets of $\mathrm{RM}(s,n)$ in $\mathrm{RM}(r,n)$, where $s < r \le n$.

Let $f_1, f_2 \in \mathcal{B}_n$. We denote by $f_1 \| f_2$ the *concatenation* of f_1 and f_2, i.e.,

$$f_1 \| f_2 := (x_{n+1}+1)f_1 + x_{n+1}f_2.$$

Let $\mathbb{F}_{2^n}$ be the finite field of size 2^n. The *absolute trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be defined as

$$\mathrm{tr}_n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}},$$

where $x \in \mathbb{F}_{2^n}$. A *monomial* Boolean function is of type $\mathrm{tr}_n(\lambda x^i)$ where $\lambda \in \mathbb{F}_{2^n}^*$ and i is an integer. It is well known that the algebraic degree of a monomial Boolean function $\mathrm{tr}_n(\lambda x^i)$ is the Hamming weight of the binary representation of i [7].

The Walsh transform of the function f at $a \in \mathbb{F}_{2^n}^*$, denoted by $W_a(f)$, is defined as

$$W_a(f) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{tr}_n(ax)}.$$

The nonlinearity of the function f also can be defined as

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}} |W_a(f)|.$$

Let $\rho = (x_{i+1}, x_{i+2}, \ldots, x_n) \in \mathbb{F}_2^{n-i}$ for $1 \le i \le n-1$. Let $f(x_1, x_2, \ldots, x_n)$ be an n-variable Boolean function. f restricted to ρ, denoted by $f|_\rho : \{x_1, x_2, \ldots, x_i\} \longrightarrow \{0,1\}$, is a subfunction of f, defined as

$$f|_\rho(x_1, x_2, \ldots, x_i) = f(x_1, x_2, \ldots, x_i, \rho).$$

The *character sum* of an n-variable Boolean function, denoted by $\mathcal{F}(f)$, is defined as

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = 2^n - 2\mathrm{wt}(f).$$

One can readily verify that, for any Boolean function f, and for any $1 \le i \le n$,

$$\mathcal{F}(f) = \sum_{\rho : \{x_{i+1}, x_{i+2}, \ldots, x_n\} \in \mathbb{F}_{2^{n-i}}} \mathcal{F}(f|_\rho). \quad (1)$$

Let $D_a f$ denote by the *derivative* of the function f with respect to $a \in \mathbb{F}_{2^n}^*$, which is defined as $D_a f = f(x) + f(x+a)$. The k-th derivative of f with respect to $a_1, \ldots, a_k \in \mathbb{F}_{2^n}^*$ is denoted by $D_{a_1} \ldots D_{a_k} f$. $D_{a_1} \ldots D_{a_k} f$ can be obtained by taking such derivative on f successively.

A *quadratic* function has algebraic degree at most 2. The dimension of the *linear kernel* of a quadratic function is related to its nonlinearity.

Definition 1. *[5, page 223] Let $Q : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a quadratic function. The linear kernel of Q, denoted by $\mathcal{E}_Q$, can be defined as*

$$\mathcal{E}_Q = \mathcal{E}_0 \cup \mathcal{E}_1$$

where

$$\mathcal{E}_0 = \{b \in \mathbb{F}_{2^n} \mid D_bQ(x) = Q(x) + Q(x+b) = 0\},$$

for all $x \in \mathbb{F}_{2^n}$;

$$\mathcal{E}_1 = \{b \in \mathbb{F}_{2^n} \mid D_bQ(x) = Q(x) + Q(x+b) = 1\},$$

for all $x \in \mathbb{F}_{2^n}$.

Lemma 2. *[5, page 224] Let $Q : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an n-variable Boolean function of degree at most 2. We denote the dimension of the* linear kernel *of Q by k. For any $\mu \in \mathbb{F}_{2^n}$, we have*

$$W_Q(\mu) \in \{0, \pm 2^{\frac{n+k}{2}}\}.$$

Carlet [6] proposed a method to estimate the lower bound on the r-th order nonlinearity of any n-variable Boolean function depending on the $(r-1)$-th order nonlinearity of all its derivatives.

Proposition 1. *[6, Proposition 3] Let f be any n-variable Boolean function and r a positive integer smaller than n. We have*

$$\mathrm{nl}_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-1}(D_a f)}.$$

3. Fourquet List-Decoding Algorithm

In the following, we give an overview of the Fourquet algorithm [10]. Given any target function f, and any $0 < \delta < 1$, the Fourquet list-decoding algorithm can output all codewords $g \in \mathrm{RM}(r,n)$ such that $\mathrm{d}(f,g) \leq 2^{n-1}(1-\delta)$. The running time is not necessarily polynomial in the block size, i.e., 2^n. Practically, given a large decoding radius, decoding RM(2, 11) or RM(3, 8) takes a lot time for a personal computer.

The key idea of the Fourquet algorithm is to write the potential codeword $g \in \mathrm{RM}(r,n)$ in its *prefix representation* and construct prefix functions of the codeword g in a recursive way.

Definition 2. *(Prefix representation) Let $g \in \mathrm{RM}(r,n)$. Boolean function g can be uniquely represented as*

$$g = g_0 + \sum_{i=1}^{n} x_i g_i(x_{i+1}, x_{i+2}, \ldots, x_n), \tag{2}$$

where $g_0 = g(0)$ and $g_i(x_{i+1}, \ldots, x_n) \in \mathrm{RM}(r-1, n-i)$. The i-th prefix function *of g is defined as*

$$g^{(i)} = \sum_{j=1}^{i} x_j g_j(x_{j+1}, x_{j+2}, \ldots, x_n).$$

In particular, $g = g^{(n)}$ or $g = g^{(n)} + 1$.

2. *Criterion*

Lemma 3. *(Lemma 2 in [10]) Let $g \in \mathrm{RM}(r,n)$, and let $g^{(i)}$ be an i-th prefix function of g. We have*

$$\mathcal{F}(f+g) \leq \sum_{\rho:\{x_{i+1}, x_{i+2}, \ldots, x_n\} \in \mathbb{F}_{2^{n-i}}} |\mathcal{F}(f|_\rho + g^{(i)}|_\rho)|.$$

For convenience, let

$$\Gamma_f(g^{(i)}) = \sum_{\rho:\{x_{i+1}, x_{i+2}, \ldots, x_n\} \in \mathbb{F}_{2^{n-i}}} |\mathcal{F}(f|_\rho + g^{(i)}|_\rho)|. \tag{3}$$

All possible valid i-th prefix functions $g^{(i)}$ satisfying $\Gamma_f(g^{(i)}) \geq 2^n\delta$ can be constructed by the Fourquet algorithm in a recursive way.

3. *How to compute $\mathcal{F}(f|_\rho + g^{(i)}|_\rho)$ for $\rho : \{x_{i+1}, \ldots, x_n\} \in \mathbb{F}_{2^{n-i}}$?*

In the Fourquet algorithm, one can use an array F_i of size 2^{n-i} to store the value of $\mathcal{F}(f|_\rho + g^{(i)}|_\rho)$ for all $\rho \in \mathbb{F}_{2^{n-i}}$, that is,

$$F_i[\rho] = \mathcal{F}(f|_\rho + g^{(i)}|_\rho).$$

Since $g^{(i)} = g^{(i-1)} + x_i g_i(x_{i+1}, x_{x+2}, \ldots, x_n)$, Fourquet deduced that

$$\begin{aligned}
&\mathcal{F}(f|_\rho + g^{(i)}|_\rho) \\
&= \mathcal{F}(f|_\rho + (g^{(i-1)} + x_i g_i(x_{i+1}, x_{x+2}, \ldots, x_n))|_\rho) \\
&= \mathcal{F}(f|_{\{x_i \leftarrow 0\}\cup\rho} + g^{(i-1)}|_{\{x_i \leftarrow 0\}\cup\rho}) \\
&\quad + \mathcal{F}(f|_{\{x_i \leftarrow 1\}\cup\rho} + g^{(i-1)}|_{\{x_i \leftarrow 1\}\cup\rho} + g_i(\rho)) \\
&= \mathcal{F}(f|_{\{x_i \leftarrow 0\}\cup\rho} + g^{(i-1)}|_{\{x_i \leftarrow 0\}\cup\rho}) \\
&\quad + (-1)^{g_i(\rho)}\mathcal{F}(f|_{\{x_i \leftarrow 1\}\cup\rho} + g^{(i-1)}|_{\{x_i \leftarrow 1\}\cup\rho}).
\end{aligned} \tag{4}$$

According to (4), one has

$$F_i[\rho] = F_{i-1}[(0,\rho)] + (-1)^{g_i(\rho)} F_{i-1}[(1,\rho)]. \tag{5}$$

4. Implementation

In our work, we implement the Fourquet-Tavernier algorithm and the Fourquet algorithm using some optimization strategies. Using these algorithms, we compute the second-order nonlinearity for some Boolean functions on $n \leq 11$ variables and compute the third-order nonlinearity for some Boolean functions on $n \leq 8$ variables. Note that the number of codewords that list-decoding algorithm for the target function outputs is zero if the decoding distance is less than its r-th order nonlinearity. Our strategy is determining the minimum value d between $[0, 2^n]$ such that there exists a codeword within distance d from the target function.

To reduce the amount of calculation, our calculation strategy uses the following optimizations:

- We use *binary search* to determine its r-th order nonlinearity between $[0, 2^n]$. Moreover, we further restrict the search space using Lemma 1, which says the distance d between the target Boolean function $f \in \mathrm{RM}(k,n)$ and any codeword $g \in \mathrm{RM}(r,n)$ must satisfy

$$d \equiv \mathrm{wt}(f) \pmod{2^{\lceil \frac{n-r}{k} \rceil}}. \tag{6}$$

So we only select the values satisfying (6) as the decoding distance in the binary search.

- In the Fourquet-Tavernier algorithm and the Fourquet algorithm, we exit the recursive search once *one* codeword is found which lies at the distance d from the target function, since our goal is to compute the r-th order nonlinearity for an n-variable Boolean function instead of list decoding.
- In the Fourquet-Tavernier algorithm, we deploy a best-first search strategy. For any valid $(i-1)$-th prefix $q^{(i-1)}$, once all valid i-th prefixes $q^{(i)} = q^{(i-1)} + x_i q_i$ are found, we expand with the most promising prefix, that is, the prefix with the maximum $\Gamma^i(q_i)$ [9, (9)].

5. Numerical Results

For the second-order nonlinearity, using the Fourquet-Tavernier algorithm, we find some 11-variable monomial Boolean functions of type $\mathrm{tr}_{11}(x^d)$ achieving the second-order nonlinearity 856 shown in Table 2. So Theorem 1 can be concluded.

Using the Fourquet algorithm, we compute the third-order nonlinearity of all n-variable monomial Boolean functions for $n = 7, 8$. It is already known that $\rho(3,8) \geq 50$ [20]. We found some quartic monomial Boolean functions of type $\mathrm{tr}_8(\lambda x^d)$ for $\lambda \in \mathbb{F}_{2^8}$ with third-order nonlinearity 56. Besides, Langevin and Leander [20] classified all non-equivalent cosets of RM(3, 8) in RM(4, 8). We compute the third-order nonlinearity of 999 non-equivalent cosets of RM(4, 8)/RM(3, 8) and find that the largest third-order nonlinearity among these cosets is 56. So Theorem 2 can be concluded. For example, the following two representative cosets have third-order nonlinearity 56:

$$x_2x_3x_4x_5 + x_1x_2x_4x_6 + x_1x_3x_5x_6 + x_2x_4x_6x_7 + x_3x_4x_6x_7 + x_2x_5x_6x_7 + x_1x_3x_4x_8 + x_1x_2x_5x_8 + x_2x_4x_7x_8 + x_1x_6x_7x_8.$$

$$x_2x_3x_4x_5 + x_1x_2x_4x_6 + x_1x_3x_5x_6 + x_2x_4x_6x_7 + x_3x_4x_6x_7 + x_2x_5x_6x_7 + x_1x_2x_3x_8 + x_1x_3x_4x_8 + x_1x_2x_5x_8 + x_1x_3x_5x_8 + x_1x_2x_6x_8 + x_2x_5x_6x_8 + x_2x_4x_7x_8 + x_3x_5x_7x_8 + x_1x_6x_7x_8.$$

So we complete the proof of Theorem 2.

Using a personal computer with 1.4 GHz Intel Core i5 and 16 GB RAM, it takes about 11.5 hours to compute the third-order nonlinearity for a monomial Boolean function on 8 variables given in Table 3 using the Fourquet algorithm. As for using the Fourquet-Tavernier algorithm to compute the second-order nonlinearity of the function $\mathrm{tr}_{11}(x^7)$, it takes about 6 days.

Table 2 Numerical results on $\rho(2, 11)$.

n	**functions**	nl_2 **lower bound**
11	$\mathrm{tr}_{11}(x^7)$,$\mathrm{tr}_{11}(x^{21})$,$\mathrm{tr}_{11}(x^{517})$, $\mathrm{tr}_{11}(x^{641})$,$\mathrm{tr}_{11}(x^{1027})$,$\mathrm{tr}_{11}(x^{1537})$	856

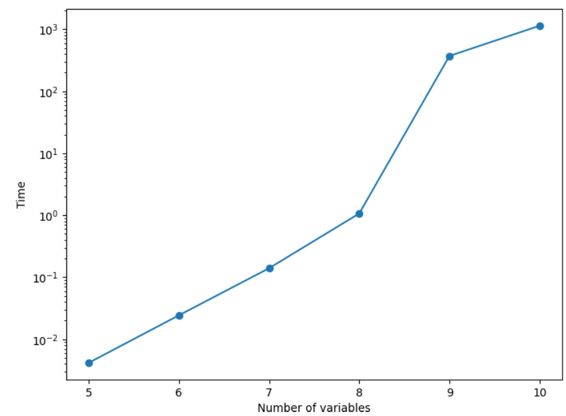

Fig. 1 Maximum time to compute nl_2 for any n-variable monomial Boolean function.

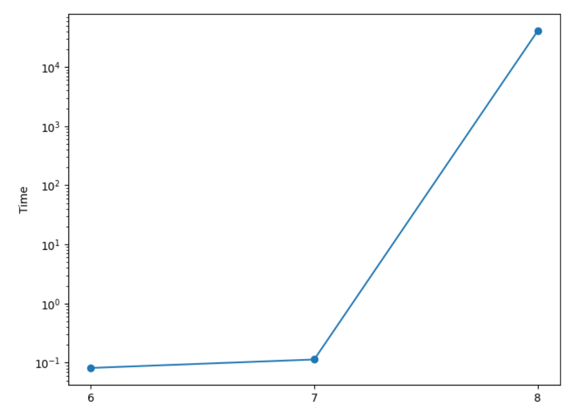

Fig. 2 Maximum time to compute nl_3 for any n-variable monomial Boolean function.

In Fig. 1, we draw a semi-log plot to observe the maximum time to compute the second-order nonlinearity for monomial Boolean functions on $n \leq 10$ variables using the Fourquet-Tavernier algorithm. Figure 2 is a semi-log plot to show the maximum time to compute the third-order nonlinearity for monomial Boolean functions on $n \leq 8$ variables using the Fourquet algorithm.

We traverse all 7-variable monomial Boolean functions and find 2540 quartic functions with third-order nonlinearity 20. Among all 8-variable monomial functions, there are 136 quartic functions with third-order nonlinearity 56. In Table 3, we summarize some quartic functions with large third-order nonlinearities.

Table 3 Numerical results on $\rho(3,n)$.

	Function	nl_3
n=7	$\mathrm{tr}_7(\lambda x^{15})$, $\mathrm{tr}_7(\lambda x^{23})$, $\mathrm{tr}_7(\lambda x^{27})$, ...	20
	Total number of monomials	
	2540	
n=8	**Function**	nl_3
	$\mathrm{tr}_8(\lambda_1 x^{15})$, $\mathrm{tr}_8(\lambda_1 x^{45})$, $\mathrm{tr}_8(\lambda_1 x^{75})$, $\mathrm{tr}_8(\lambda_1 x^{105})$, $\mathrm{tr}_8(\lambda_1 x^{135})$, $\mathrm{tr}_8(\lambda_1 x^{165})$, $\mathrm{tr}_8(\lambda_1 x^{195})$, $\mathrm{tr}_8(\lambda_1 x^{225})$	56
	Total number of monomials	
	136	

(1) $\lambda \in \mathbb{F}_{2^7}^*$;

(2) $\lambda_1 \in \{ 1, 8, 29, 47, 53, 54, 57, 64, 74, 99, 102, 171, 179, 194, 211, 232, 239 \}$

6. Complexity

In [10], given the decoding radius up to the Johnson bound, it is proved that the complexity of the Fourquet algorithm is linear in the length of the code 2^n. We will prove that there exists an n-variable Boolean function f such that the Fourquet algorithm can find all codewords in $\mathrm{RM}(r,n)$ within $2^{n-r}-\epsilon$ for $\epsilon > 0$ from f with linear complexity in 2^n.

We will need the following theorem in the proof of Theorem 3.

Theorem 5. *[3, Theorem 1] Let $\mathbb{F}_q$ denote by the finite field of size q. Let $\mathcal{P}_r(\mathbb{F}_q^n)$ be the set of the polynomials $g : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ of degree $\le r$. Let $\ell_{\mathbb{F}_q}(r,n,d)$ denote by the maximum number of functions $g \in \mathcal{P}_r(\mathbb{F}_q^n)$ within distance d from f for any function $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$. Let $\epsilon > 0$ and $r,n \in \mathbb{N}$. Then we have*

$$\ell_{\mathbb{F}_q^n}(r,n,2^{n-r}-\epsilon) \le c_{q,r,\epsilon},$$

where $c_{q,r,\epsilon}$ is a constant.

Now we are ready to prove Theorem 3.

Proof. (of Theorem 3) Let $\gamma_{r,n}$ denote by the complexity of the Fourquet algorithm. $\gamma_{r,n}$ can be defined as follows [10]:

$$\gamma_{r,n} = \quad O(2^n \cdot l^r), \tag{7}$$

where l is the upper bound of the number of the i-th prefix functions that the Fourquet algorithm outputs at step i for $1 \le i \le n$.

Let $f = f_1 \| f_2 \in \mathrm{RM}(r+1,n)$ for $f_1 = 0$, $f_2 \in \mathrm{RM}(r,n-1)$ with $\mathrm{nl}_{r-1}(f_2) = 2^{n-r}-\epsilon$ for $\epsilon > 0$. Applying the affine transformation $x_i \longrightarrow x_{n+1-i}$ to f for all $1 \le i \le n$, we get a new Boolean function, denoted by $f' \in \mathrm{RM}(r+1,n)$. Let $p = \sum_{j=1}^{i} x_j p_j(x_{j+1},x_{j+2},\ldots,x_n) + p_{\mathrm{suff}}(x_{i+1},x_{i+2},\ldots,x_n)$, where $p_j \in \mathrm{RM}(r-1,n-j)$ and $p_{\mathrm{suff}} \in \mathcal{B}_{n-i}$. The i-th prefix function of the function p is defined as $p^{(i)} = \sum_{j=1}^{i} x_j p_j(x_{j+1},x_{j+2},\ldots,x_n) \ne 0$ for $p_j \in \mathrm{RM}(r-1,n-j)$. Given any decoding radius $d = 2^{n-r}-\epsilon_1$ for $0 < \epsilon_1 \le \epsilon$, let S denote by the set of all the functions p such that $\mathrm{d}(f',p) \le 2^{n-r}-\epsilon_1$ for $0 < \epsilon_1 \le \epsilon$.

In the following, we will prove that the number of all i-th prefix functions $p^{(i)}$ of all functions $p \in S$ is upper bounded by a constant.

Let $p' = g\|g + p'_n$ be such that $\mathrm{d}(f,p') \le 2^{n-r} - \epsilon_1$ for $g = \sum_{j=n-1}^{j=n+1-i} x_j p'_j(x_{j-1},x_{j-2},\ldots,x_1) + p'_{\mathrm{suff}}$ and $p'_n(x_1,x_2,\ldots,x_{n-1}) \in \mathrm{RM}(r-1,n-1)$, where $p'_j \in (r-1,j-1)$, $p'_{\mathrm{suff}} \in \mathcal{B}_{n-i}$ and $1 \le i \le n$. The $i-1$-th prefix function of the function g is defined as $g^{(i-1)} = \sum_{j=n-1}^{j=n+1-i} x_j p'_j(x_{j-1},x_{j-2},\ldots,x_1) \ne 0$ for $p'_j \in \mathrm{RM}(r-1,j-1)$. Let T denote by the set of all functions p' such that $\mathrm{d}(f,p') \le 2^{n-r}-\epsilon_1$, that is, $T = \{p' \mid \mathrm{d}(f,p') \le 2^{n-r}-\epsilon_1\}$.

Note that

$$\begin{aligned} &\mathrm{d}(f,p') \\ =\ &\mathrm{d}(f_1\|f_2, g\|g+p'_n) \\ =\ &\mathrm{wt}(f_1+g) + \mathrm{wt}(f_2+g+p'_n). \end{aligned} \tag{8}$$

Since $\mathrm{wt}((f_1+g)+(f_2+g+p'_n)) = \mathrm{wt}(f_1+f_2+p'_n) = \mathrm{wt}(f_1+g)+\mathrm{wt}(f_2+g+p'_n) - 2\mathrm{wt}((f_1+g)(f_2+g+p'_n))$, by (8), we have

$$\begin{aligned} &\mathrm{d}(f,p') \\ =\ &\mathrm{wt}(f_1+g)+\mathrm{wt}(f_2+g+p'_n) \\ =\ &\mathrm{wt}(f_1+f_2+p'_n) + 2\mathrm{wt}((f_1+g)(f_2+g+p'_n)). \end{aligned} \tag{9}$$

Since $\mathrm{d}(f,p') \le 2^{n-r}-\epsilon_1$, by (9), we can deduce that $\mathrm{nl}_{r-1}(f_1+f_2) \le \mathrm{wt}(f_1+f_2+p'_n) \le 2^{n-r}-\epsilon_1$. By Theorem 5, we can deduce that the number of functions $p'_n \in \mathrm{RM}(r-1,n-1)$ such that $\mathrm{d}(f_1+f_2,p'_n) \le 2^{n-r}-\epsilon_1$ for any $\epsilon_1 > 0$ is upper bounded by a constant c_{2,r,ϵ_1}, which is independent of n.

Let $\rho' : \{x_1,x_2,\ldots,x_{n-i}\} \in \mathbb{F}_2^{n-i}$ for $2 \le i \le n-1$. We have $g|_{\rho'} \in \mathrm{RM}(r,i-1)$. If there exists a vector $\rho' \in \mathbb{F}_2^{n-i}$ such that $\deg(g|_{\rho'}) = r$, we can deduce that $\deg(g|_{\rho'}) = r$ holds for all $\rho' \in \mathbb{F}_2^{n-i}$ and the ANFs of all functions $g|_{\rho'}$ contain the same sum of the monomials of degree r. Note that the minimum weight of the r-th order Reed-Muller code $\mathrm{RM}(r,i-1)$ is 2^{i-r-1}. Since $\mathrm{wt}(g) = \sum_{\rho' \in \mathbb{F}_2^{n-i}} \mathrm{wt}(g|_{\rho'})$, we can deduce that $\mathrm{wt}(g) \ge 2^{i-r-1} \cdot 2^{n-i} = 2^{n-r-1}$ when $\deg(g|_{\rho'}) = r$. Since $g^{(i-1)} \ne 0 \in \mathrm{RM}(r,n-1)$, if there exists an vector $\rho' \in \mathbb{F}_2^{n-i}$ such that $1 \le \deg(g|_{\rho'}) = t < r$, we can deduce that there exist at least $2^{n-i-r+t}$ vectors $\rho' \in \mathbb{F}_2^{n-i}$ such that $\mathrm{wt}(g|_{\rho'}) \ge 2^{i-t-1}$. Hence, we have $\mathrm{wt}(g) = \sum_{\rho' \in \mathbb{F}_2^{n-i}} \mathrm{wt}(g|_{\rho'}) \ge 2^{i-t-1} \cdot 2^{n-i-r+t} = 2^{n-r-1}$.

In the same way, we can deduce that $\mathrm{wt}(f_2+g+p'_n) \ge 2^{n-r-1}$. Hence, we have $\mathrm{d}(f,p') = \mathrm{wt}(f_1+g) + \mathrm{wt}(f_2+g+p'_n) = \mathrm{wt}(g) + \mathrm{wt}(f_2+g+p'_n) \ge 2^{n-r}$, which is a contradiction. Therefore, we can deduce that $g = 0$ or $g = \sum_{j=i_0}^{1} x_j g_j(x_{j-1},x_{j-2},\ldots,x_1)$ for $\deg(g_{i_0}) \ge r$ and $g^{(i_0-1)} = 0$, where $1 \le i_0 \le n-1$.

Since the function f' is affine equivalent to f under the action of the affine transformation $x_i \to x_{n-i+1}$ for all $1 \le i \le n$, the set S can be obtained by applying the affine transformation $x_i \to x_{n-i+1}$ for all $1 \le i \le n$ on each element of the set T. Hence, we can deduce that any function $p \in S$ must satisfy that $p = x_1 p_1(x_2, x_3, \ldots, x_n)$ for $p_1 \in \mathrm{RM}(r-1, n-1)$, or $p = x_1 p_1(x_2, x_3, \ldots, x_n) + \sum_{j=i_0}^{n} x_j p_j(x_{j+1}, x_{j+2}, \ldots, x_n)$ for $p_1 \in \mathrm{RM}(r-1, n-1)$ and $\deg(p_{i_0}) \ge r$, where $2 \le i_0 \le n$. Moreover, we can deduce that the number of functions p_1 is upper bounded by c_{2,r,ϵ_1}. Hence, we have $l \le c_{2,r,\epsilon_1}$ for any $1 \le i \le n$, where c_{2,r,ϵ_1} is a constant.

Since $l \le c_{2,r,\epsilon_1}$, by (7), we have $\gamma_{r,n} = O(2^n)$ for $r \ll n$. □

7. Third-Order Nonlinearity

Applying Proposition 1 twice, we have the following proposition.

Proposition 2. *[6, page 1265] Let $f \in \mathcal{B}_n$ and r a positive integer. Then we have*

$$\mathrm{nl}_r(f) \ge 2^{n-1} - \frac{1}{2}\sqrt{\sum_{a \in \mathbb{F}_{2^n}} \sqrt{2^{2n} - 2\sum_{b \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-2}(D_a D_b f)}}.$$

Note that

$$\sum_{b \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-2}(D_a D_b f) = \sum_{b \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-2}(D_a D_{ab} f) = \sum_{b \in \mathbb{F}_{2^n}} \mathrm{nl}_{r-2}(D_{ab} D_a f)$$

for any $a \in \mathbb{F}_{2^n}$ [12]. To lower-bound the third order nonlinearity of $f = \mathrm{tr}_n(x^{15})$, by Proposition 2, the central object is to estimate the nonlinearities of $D_{ab}D_a f$ for all $a, b \in \mathbb{F}_{2^n}$, which is equivalent to calculate the dimension of the linear kernel of $D_{ab}D_a f$. In fact, this target is equivalent to analyzing the number of the roots of a polynomial (related to the linear kernel) over a finite field. In [12], to analyze the number of roots of the complex polynomial, they factor the polynomial into irreducible polynomials and estimate the number of roots of each component. Inspired by the work in [12], we have a more accurate estimate of the number of roots of the polynomial, which is related to the linear kernel of $D_{ab}D_a f$. Hence, we slightly improve the best proven lower bound on the third-order nonlinearity of $\mathrm{tr}_n(x^{15})$.

The following lemmas will be used in the proof of Theorem 4.

Lemma 4. *[12, Lemma 6] Let $f = \mathrm{tr}_n(x^{15})$. Let $\dim(\mathcal{E}_f)$ denote by the dimension of $\mathcal{E}_f$. Let $g = D_{ab}D_a f(ax)$. Note that $\dim(\mathcal{E}_g) = \dim(\mathcal{E}_{D_{ab}D_a f})$ for any fixed $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$. The element $x \in \mathbb{F}_{2^n}^*$ satisfies $x \in \mathcal{E}_g$ if and only if $P(x, a, b) = 0$, where*

$$P(x, a, b) = Q(x, a, b)(Q(x, a, b) + 1)$$

and

$$Q(x, a, b) = (b^2 + b)^{-4} R(x, a, b)(R(x, a, b) + 1).$$

and

$$\begin{aligned} &R(x, a, b) \\ =&a^{30}(b^2 + b)^6 \left((x^2 + x)^2 + (x^2 + x)(b^2 + b)\right)^4 \\ &+ a^{15}(b^2 + b)^5 \left((x^2 + x)^2 + (x^2 + x)(b^2 + b)\right). \end{aligned}$$

Lemma 5. *[12, Lemma 7] For any fixed $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, the number of the roots of $P(x, a, b) = 0$ can be 2^k for $k = 2, 4, 6$, when n is even; the number of the roots of $P(x, a, b) = 0$ can be 2^k for $k = 3, 5$, when n is odd.*

Lemma 6. *[12, Lemma 9] Let $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$. When the number of the roots of $R(x, a, b) = 0$ equals 4, the number of the roots of $P(x, a, b) = 0$ is at most 8 for odd n.*

In this paper, we improve the lower bound on the number of $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $\dim(\mathcal{E}_{D_{ab}D_a f}) \le 4$ for any fixed $a \in \mathbb{F}_{2^n}^*$.

7.1 For Even n

Theorem 6. *Let $f = \mathrm{tr}_n(x^{15})$ and even n. We denote the dimension of $\mathcal{E}_{D_{ab}D_a f}$ by $\dim(\mathcal{E}_{D_{ab}D_a f})$. For any fixed $a \in \mathbb{F}_{2^n}^*$, we have the distribution of $\dim(\mathcal{E}_{D_{ab}D_a f})$ as follows:*

Table 4 The distribution of $\dim(\mathcal{E}_{D_{ab}D_a f})$ for any fixed $a \in \mathbb{F}_{2^n}^*$ and even n.

$\dim(\mathcal{E}_{D_{ab}D_a f})$	The number of elements $b \in \mathbb{F}_{2^n}$
n	2
$\{2, 4\}$	$\ge \frac{1}{3}(2^n - 4 + \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$
6	$\le \frac{1}{3}(2^{n+1} - 2 - \mathrm{wt}(\mathrm{tr}_n(x^3)) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})))$

Proof. For $b \notin \{0, 1\}$, since $R(x, a, b) = 0$, we can deduce that $(x^2+x)^2 + (x^2+x)(b^2+b) = 0$ for $x \in \{0, 1, b, b+1\}$ or

$$((x^2 + x)^2 + (x^2 + x)(b^2 + b))^3 = \frac{1}{a^{15}(b^2 + b)} \tag{10}$$

for $x \notin \{0, 1, b, b+1\}$. When $x \in \{0, 1, b, b+1\}$, let $G = \{g^{3s} \mid 0 \le s \le \frac{2^n-4}{3}\}$ be the multiplicative group of order $\frac{2^n-1}{3}$, where g is a primitive element. If $b^2 + b \notin G$, we can deduce that (10) has no solution. That is, the number of roots of $R(x, a, b) = 0$ is at most 4. It is proved that the number of elements $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $b^2 + b \notin G$ is $\frac{1}{3}(2^n - 4 + 2\mathrm{wt}(\mathrm{tr}_n(x^3)))$ [12].

When $b^2 + b \in G$, we will lower-bound the number of the elements $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $R(x, a, b) = 0$ has < 16 solutions. Since $x \in \{0, 1, b, b+1\}$ are four roots of $R(x, a, b) = 0$, we need to lower-bound the number of the elements $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that (10) has < 12 solutions.

Let $c^3 = b^2 + b$, where $c \in \mathbb{F}_{2^n}^*$. Then we have

$$\left(\frac{1}{a^{15}(b^2+b)}\right)^{\frac{1}{3}} = a^{-5}c^{-1}.$$

According to (10), we have

$$(x^2+x)^2 + (x^2+x)c^3 = a^{-5}c^{-1}. \tag{11}$$

Multiplying both sides of (11) by $\frac{1}{c^6}$, we have

$$\left(\frac{x^2+x}{c^3}\right)^2 + \frac{x^2+x}{c^3} = a^{-5}c^{-7}. \tag{12}$$

Let $z = \frac{x^2+x}{c^3}$. According to (12), we have

$$z^2 + z = a^{-5}c^{-7} = a^{2^n-6}c^{2^n-8}.$$

There exist two solutions of the above equation if and only if $\mathrm{tr}_n(a^{2^n-6}c^{2^n-8}) = 0$. If $c^3 = b^2+b$ and $\mathrm{tr}_n(a^{2^n-6}c^{2^n-8}) = 1$ hold for any $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$ and any fixed $a \in \mathbb{F}_{2^n}^*$, we can deduce that (12) has no solution, that is, (10) has no solution. Then the number of the roots of $R(x,a,b) = 0$ is < 16. For any $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$, the equation $c^3 = b^2+b$ holds if and only if $\mathrm{tr}_n(c^3) = 0$. Then for all $c \in \mathbb{F}_{2^n}^*$ and any fixed $a \in \mathbb{F}_{2^n}^*$, the number of the elements $c \in \mathbb{F}_{2^n}^*$ such that $\mathrm{tr}_n(c^3) = 0$ and $\mathrm{tr}_n(a^{2^n-6}c^{2^n-8}) = 1$ is $\frac{1}{2}(\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$. Since $c \mapsto c^3$ is a 3-to-1 mapping over $\mathbb{F}_{2^n}^*$, then the number of the elements c^3 such that $\mathrm{tr}_n(c^3) = 0$ and $\mathrm{tr}_n(a^{2^n-6}c^{2^n-8}) = 1$ is at least

$$\frac{1}{6}(\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3))).$$

Since $b \mapsto b^2+b$ is a 2-to-1 mapping over $\mathbb{F}_{2^n} \setminus \{0,1\}$, then we can deduce that the number of elements $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$ such that $c^3 = b^2+b \in G$ and $\mathrm{tr}_n(a^{2^n-6}c^{2^n-8}) = 1$ is at least $\frac{1}{3}(\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$. Combining the case of $b^2+b \notin G$, we have the number of elements $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$ such that $R(x,a,b) = 0$ has < 16 solutions is at least

$$\begin{aligned}&\frac{1}{3}(2^n - 4 + 2\mathrm{wt}(\mathrm{tr}_n(x^3))) + \\ &\frac{1}{3}(\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(x^3)) \\ &+ \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3))) \\ = &\frac{1}{3}(2^n - 4 + \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) \\ &+ \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3))).\end{aligned} \tag{13}$$

Let s_{R_0} denote by the number of the solutions of $R(x,a,b) = 0$, s_{R_1} denote by the number of solutions of $R(x,a,b)+1 = 0$, s_{Q_0} denote by the number of the solutions of $Q(x,a,b) = 0$, s_{Q_1} denote by the number of the solutions of $Q(x,a,b)+1 = 0$, s_P denote by the number of the solutions of $P(x,a,b) = 0$. According to Lemma 4, since $\deg(R(x,a,b)+1) = 16$, we have $s_{Q_0} = s_{R_0} + s_{R_1} \le s_{R_0} + 16$. Since $\deg(Q(x,a,b)+1) = 32$, we have $s_P = s_{Q_0} + s_{Q_1} \le s_{Q_0} + 32$. For $s_{R_0} < 16$, we can deduce that $s_P < 64$. By Lemma 5, we have $s_P \le 16$ for $s_{R_0} < 16$. Hence, we can deduce that the number of elements $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$ such that $\dim(\mathcal{E}_{D_{ab}D_af}) \le 4$ is at least $\frac{1}{3}(2^n - 4 + \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$; the number of elements $b \in \mathbb{F}_{2^n} \setminus \{0,1\}$ such that $\dim(\mathcal{E}_{D_{ab}D_af}) = 6$ is at most $\frac{1}{3}(2^{n+1} - 2 - \mathrm{wt}(\mathrm{tr}_n(x^3)) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})))$. □

Table 5 The distribution of $\mathrm{nl}(D_{ab}D_af)$.

$\mathrm{nl}(D_{ab}D_af)$	The number of elements $b \in \mathbb{F}_{2^n}$
0	2
$\ge 2^{n-1} - 2^{\frac{n}{2}+1}$	$\ge \frac{1}{3}(2^n - 4 + \mathrm{wt}(\mathrm{tr}_n(x^3)) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) + \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$
$2^{n-1} - 2^{\frac{n}{2}+2}$	$\le \frac{1}{3}(2^{n+1} - 2 - \mathrm{wt}(\mathrm{tr}_n(x^3)) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) - \mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)))$

According to Lemma 2 and Theorem 6, we have the following corollary.

Corollary 1. *Let $f(x) = \mathrm{tr}_n(x^{15})$. Let $\mathrm{nl}(D_{ab}D_af)$ denote by the nonlinearity of $D_{ab}D_af$. For any $b \in \mathbb{F}_{2^n}$ and even n, the distribution of $\mathrm{nl}(D_{ab}D_af)$ is as follows:*

Let $\mathcal{X}$ denote by the nontrivial additive character over $\mathbb{F}_q$, where $q = p^n$. For $p = 2$, we have $\mathcal{X}(x) = e^{\frac{2\pi i \mathrm{tr}_n(x)}{p}} = (-1)^{\mathrm{tr}_n(x)}$[19].

Theorem 7. *[19, Weil bound, Theorem 5.38] Let $f(x) \in \mathbb{F}_q[x]$ with degree $d \ge 1$, where $\gcd(d,q) = 1$. We have*

$$\left|\sum_{x \in \mathbb{F}_q} \mathcal{X}(f(x))\right| \le (d-1)q^{\frac{1}{2}}.$$

As an extension of Weil bound, the Kloosterman sum is the character sum of the function of type $\lambda \cdot \frac{1}{x} + ax$ over $\mathbb{F}_{2^n}$, which is defined as $\sum_{x \in \mathbb{F}_{2_n}} (-1)^{\mathrm{tr}_n(\lambda \cdot \frac{1}{x} + ax)}$ for any $\lambda, a \in \mathbb{F}_{2^n}^*$. The extended Kloosterman sum over Galois rings is upper bounded by Shanbhag et al. [25]. By Theorem 1 in [25], we have the following theorem.

Theorem 8. *[25, Theorem 1] Let $f(x), g(x) \in \mathbb{F}_{2^n}[x]$ be two univariate polynomials of odd degree. We have*

$$\left|\sum_{x \in \mathbb{F}_{2^n}} \mathcal{X}(f(x) + g(x^{-1}))\right| \le (\deg(f) + \deg(g)) \cdot 2^{\frac{n}{2}}.$$

The following lemma shows the concrete results on the character sums of the function $x^3 \in \mathbb{F}_{2^n}$ for even n.

Lemma 7. *[4] Let $G = \{g^{3s} \mid 0 \le s \le \frac{2^n-4}{3}\}$ be a multiplicative group of order $\frac{2^n-1}{3}$, where g is a primitive element. For even n and any $\lambda \in \mathbb{F}_{2^n}^*$, there exists*

$$\sum_{x\in\mathbb{F}_{2^n}} \mathcal{X}(\lambda x^3) = \begin{cases} (-1)^{\frac{n}{2}+1}2^{\frac{n}{2}+1}, & \textit{if } \lambda \in G \\ (-1)^{\frac{n}{2}}2^{\frac{n}{2}}, & \textit{if } \lambda \notin G \end{cases}.$$

According to Lemma 7, we can deduce that

$$\mathrm{wt}(\mathrm{tr}_n(x^3)) = \begin{cases} 2^{n-1} - 2^{\frac{n}{2}}, & \text{if } 4 \nmid n \\ 2^{n-1} + 2^{\frac{n}{2}}, & \text{if } 4 \mid n \end{cases}. \tag{14}$$

Note that $\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3) = \mathrm{tr}_n(a^{2^n-6}(\frac{1}{x})^7 + x^3)$. By Theorem 8, we can deduce that

$$\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8} + x^3)) \geq 2^{n-1} - 5 \cdot 2^{\frac{n}{2}}. \tag{15}$$

We will discuss the value of $\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8}))$ in the following two cases.

Case 1: $3 \nmid n$, we have $\gcd(2^n - 8, 2^n - 1) = 1$. Note that $x \mapsto ax$ is a bijection over $\mathbb{F}_{2^n}$ for any $a \in \mathbb{F}^*_{2^n}$, we have $x \mapsto a^{2^n-6}x^{2^n-8}$ is also bijection over $\mathbb{F}_{2^n}$. Then we have $\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) = \mathrm{wt}(\mathrm{tr}_n(x)) = 2^{n-1}$.

Case 2: $3 \mid n$. Since $\gcd(2^n - 8, 2^n - 1) = 7$ and $\gcd(\frac{2^n-8}{7}, \frac{2^n-1}{7}) = 1$, we have $x \mapsto x^{\frac{2^n-8}{7}}$ is bijection over $\mathbb{F}_{2^n}$. Note that $\mathrm{tr}_n(\lambda x^{2^n-8}) = \mathrm{tr}_n(\lambda(x^{\frac{2^n-8}{7}})^7)$ for any $\lambda \in \mathbb{F}_{2^n}$. Then we can deduce that the number of elements $x \in \mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(\lambda x^{2^n-8}) = 1$ equals the number of $x \in \mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(\lambda x^7)$ for $\lambda \in \mathbb{F}_{2^n}$. By Theorem 7, we can deduce that $\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) \geq 2^{n-1} - 3 \cdot 2^{\frac{n}{2}}$ for any fixed $a \in \mathbb{F}^*_{2^n}$.

Hence, we have

$$\mathrm{wt}(\mathrm{tr}_n(a^{2^n-6}x^{2^n-8})) = \begin{cases} 2^{n-1}, & 3 \nmid n \\ \geq 2^{n-1} - 3 \cdot 2^{\frac{n}{2}}, & 3 \mid n \end{cases}. \tag{16}$$

Now we will prove the lower bound on the third-order nonlinearity of $\mathrm{tr}_n(x^{15})$, as shown in Theorem 4.

Proof. (of Theorem 4) For $3 \nmid n$, by Corollary 1, (14), (15), (16), we have the elements of $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $\mathrm{nl}(D_{ab}D_a f) \geq 2^{n-1} - 2^{\frac{n}{2}+1}$ is at least $\frac{1}{3}(5 \cdot 2^{n-1} - 6 \cdot 2^{\frac{n}{2}} - 4)$; the elements of $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $\mathrm{nl}(D_{ab}D_a f) \geq 2^{n-1} - 2^{\frac{n}{2}+2}$ is at most $\frac{1}{3}(2^{n-1} + 6 \cdot 2^{\frac{n}{2}} - 2)$.

Hence, according to Proposition 2, we can deduce that

$$\begin{aligned} &\mathrm{nl}_3(f) \\ \geq\ & 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)\sqrt{2^{2n} - 2c_1} + 2^n} \\ =\ & 2^{n-1} - \\ & \frac{1}{2}\sqrt{(2^n - 1)\sqrt{\frac{7}{3} \cdot 2^{\frac{3}{2}n+1} + 5 \cdot 2^{n+1} - \frac{1}{3} \cdot 2^{\frac{n}{2}+5}} + 2^n} \\ \geq\ & 2^{n-1} - 2^{\frac{7n}{8} - \frac{3}{4} + \frac{1}{4}\log_2 \frac{7}{3}} - O(2^{\frac{3}{8}n}), \end{aligned}$$

where

$$\begin{aligned} c_1 =& (2^{n-1} - 2^{\frac{n}{2}+1})(\frac{5 \cdot 2^{n-1} - 6 \cdot 2^{\frac{n}{2}} - 4}{3}) \\ &+ (2^{n-1} - 2^{\frac{n}{2}+2})(\frac{2^{n-1} + 6 \cdot 2^{\frac{n}{2}} - 2}{3}). \end{aligned}$$

Table 6 The distribution of $\dim(\mathcal{E}_{D_{ab}D_a f})$ for any fixed $a \in \mathbb{F}^*_{2^n}$, odd n.

$\dim(\mathcal{E}_{D_{ab}D_a f})$	The number of $b \in \mathbb{F}_{2^n}$
n	2
3	$\geq \mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))$ $+\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}} + x)) - 2^{n-1}$
5	$\leq 3 \cdot 2^{n-1} - 2 - \mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))$ $-\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}} + x))$

For $3 \mid n$, by Corollary 1, (14), (15), (16), we have the elements of $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $\mathrm{nl}(D_{ab}D_a f) \geq 2^{n-1} - 2^{\frac{n}{2}+1}$ is at least $\frac{1}{3}(5 \cdot 2^{n-1} - 9 \cdot 2^{\frac{n}{2}} - 4)$; the elements of $b \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ such that $\mathrm{nl}(D_{ab}D_a f) \geq 2^{n-1} - 2^{\frac{n}{2}+2}$ is at most $\frac{1}{3}(2^{n-1} + 9 \cdot 2^{\frac{n}{2}} - 2)$. According to Proposition 2, then we can deduce that

$$\begin{aligned} &\mathrm{nl}_3(f) \\ \geq\ & 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)\sqrt{2^{2n} - 2c_2} + 2^n} \\ =\ & 2^{n-1} - \\ & \frac{1}{2}\sqrt{(2^n - 1)\sqrt{\frac{7}{3} \cdot 2^{\frac{3}{2}n+1} + 7 \cdot 2^{n+1} - \frac{1}{3} \cdot 2^{\frac{n}{2}+5}} + 2^n} \\ =\ & 2^{n-1} - 2^{\frac{7n}{8} - \frac{3}{4} + \frac{1}{4}\log_2 \frac{7}{3}} - O(2^{\frac{3}{8}n}), \end{aligned}$$

where

$$\begin{aligned} c_2 =& (2^{n-1} - 2^{\frac{n}{2}+1})(\frac{5 \cdot 2^{n-1} - 9 \cdot 2^{\frac{n}{2}} - 4}{3}) \\ &+ (2^{n-1} - 2^{\frac{n}{2}+2})(\frac{2^{n-1} + 9 \cdot 2^{\frac{n}{2}} - 2}{3}). \end{aligned}$$

□

7.2 For Odd n

In the following, we improve the lower bound on the third-order nonlinearity of $\mathrm{tr}_n(x^{15})$ for odd n.

Theorem 9. *Let $f = \mathrm{tr}_n(x^{15})$ and n be odd. We denote by $\dim(\mathcal{E}_{D_{ab}D_a f})$ the dimension of $\mathcal{E}_{D_{ab}D_a f}$. We have*

Proof. For $R(x, a, b) = 0$ and $x \notin \{0, 1, b, b + 1\}$, we can deduce that

$$(x^2 + x)^2 + (b^2 + b)(x^2 + x) = a^{-5}(b^2 + b)^{\frac{2^n-2}{3}}. \tag{17}$$

Multiplying both sides of (17) by $\frac{1}{(b^2+b)^2}$, we have

$$\left(\frac{x^2 + x}{b^2 + b}\right)^2 + \frac{x^2 + x}{b^2 + b} = a^{-5}(b^2 + b)^{\frac{2^n-8}{3}}. \tag{18}$$

If $\mathrm{tr}_n(a^{-5}(b^2 + b)^{\frac{2^n-8}{3}}) = 1$, then there exists no solution to (18). Then there exist at most 4 solutions of $R(x, a, b) = 0$ for any fixed $a \in \mathbb{F}^*_{2^n}$. By Lemma 6, we can deduce that there

Table 7 The distribution of $\mathrm{nl}(D_{ab}D_af)$ for any fixed $a \in \mathbb{F}_{2^n}^*$, odd n.

$\mathrm{nl}(D_{ab}D_af)$	The number of $b \in \mathbb{F}_{2^n}$
0	2
$2^{n-1}-2^{\frac{n+1}{2}}$	$\geq \mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))$ $+\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))-2^{n-1}$
$2^{n-1}-2^{\frac{n+3}{2}}$	$\leq 3\cdot 2^{n-1}-2-\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))$ $-\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))$

exist at most 8 solutions of $P(x,a,b)=0$, which implies $\dim(\mathcal{E}_{D_{ab}D_af})\leq 3$. We will lower-bound the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{tr}_n(a^{-5}(b^2+b)^{\frac{2^n-8}{3}})=1$.

Note that $b^2+b=x$ has two solutions if and only if $\mathrm{tr}_n(x)=0$. We can deduce that the number of elements $x\in\mathbb{F}_{2^n}^*$ such that $\mathrm{tr}_n(x)=0$ and $\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}})=1$ is $\frac{1}{2}(\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))-\mathrm{wt}(\mathrm{tr}_n(x))+\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x)))$. Hence, the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{tr}_n(b^2+b)=0$ and $\mathrm{tr}_n(a^{-5}(b^2+b)^{\frac{2^n-8}{3}})=1$ is at least $\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))-\mathrm{wt}(\mathrm{tr}_n(x))+\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))$.

Since $\mathrm{wt}(\mathrm{tr}_n(x))=2^{n-1}$, according to Lemma 5 and Lemma 6, we can deduce that the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\dim(\mathcal{E}_{D_{ab}D_af})\leq 3$ is at least $\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))+\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))-2^{n-1}$; the number of $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\dim(\mathcal{E}_{D_{ab}D_af})=5$ is at most $3\cdot 2^{n-1}-2-\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))-\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))$. □

According to Theorem 9, we can deduce the following corollary.

Corollary 2. *Let $f=\mathrm{tr}_n(x^{15})$ and n be odd. We denote the nonlinearity of $D_{ab}D_af$ by $\mathrm{nl}(D_{ab}D_af)$. For any fixed $a\in\mathbb{F}_{2^n}$, the distribution of $\mathrm{nl}(D_{ab}D_af)$ is as follows:*

For odd n, we have $\gcd(2^n-1,3)=1$. Hence, we have $x\mapsto x^3$ is bijection over $\mathbb{F}_{2^n}$. Applying $x\mapsto x^3$ to the function $\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x)$, we have $\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))=\mathrm{wt}(\mathrm{tr}_n(a^{-5}(\frac{1}{x})^7+x^3))$.

According to Theorem 8, we can deduce that

$$\begin{aligned}&\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}+x))=\mathrm{wt}(\mathrm{tr}_n(a^{-5}(\frac{1}{x})^7+x^3))\\&\geq 2^{n-1}-5\cdot 2^{\frac{n}{2}}\end{aligned}\tag{19}$$

for any $a\in\mathbb{F}_{2^n}^*$.

Case 1: $3\nmid n$. Since $\gcd(\frac{2^n-8}{3},2^n-1)=1$, then $x\mapsto x^{\frac{2^n-8}{3}}$ is a bijection over $\mathbb{F}_{2^n}$. For any $c\in\mathbb{F}_{2^n}^*$, $x\mapsto cx$ is a bijection over $\mathbb{F}_{2^n}$. Hence, the number of the elements $x\in\mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(x)=1$ equals the number of the elements $x\in\mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}})=1$. Hence, we have $\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))=\mathrm{wt}(\mathrm{tr}_n(x))=2^{n-1}$.

Case 2: $3\mid n$. Since $\gcd(\frac{2^n-8}{3},2^n-1)=7$, then we have $x\mapsto x^{\frac{2^n-8}{3}}$ is a 7-to-1 mapping over $\mathbb{F}_{2^n}$. Note that $\gcd(\frac{2^n-8}{21},\frac{2^n-1}{7})=1$. We have $x\mapsto x^{\frac{2^n-8}{21}}$ is a bijection over $\mathbb{F}_{2^n}$. Hence, the number of elements $x\in\mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}})=\mathrm{tr}_n(a^{-5}(x^{\frac{2^n-8}{21}})^7)=1$ equals the number of elements $x\in\mathbb{F}_{2^n}$ such that $\mathrm{tr}_n(a^{-5}x^7)=1$. According to Theorem 7, we can deduce that $\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))\geq 2^{n-1}-3\cdot 2^{\frac{n}{2}}$.

Therefore, we have

$$\mathrm{wt}(\mathrm{tr}_n(a^{-5}x^{\frac{2^n-8}{3}}))=\begin{cases}2^{n-1}, & 3\nmid n\\ \geq 2^{n-1}-3\cdot 2^{\frac{n}{2}}, & 3\mid n\end{cases}.\tag{20}$$

We will prove the lower bound on the third-order nonlinearity of $\mathrm{tr}_n(x^{15})$ for odd n, as shown in Theorem 4.

Proof. (of Theorem 4) For $3\nmid n$, according to Corollary 2, (19) and (20), we can deduce that the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{nl}(D_{ab}D_af)\geq 2^{n-1}-2^{\frac{n+1}{2}}$ is at least $2^{n-1}-5\cdot 2^{\frac{n}{2}}$ for any fixed $a\in\mathbb{F}_{2^n}^*$; the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{nl}(D_{ab}D_af)\geq 2^{n-1}-2^{\frac{n+3}{2}}$ for any fixed $a\in\mathbb{F}_{2^n}^*$ is at most $2^{n-1}+5\cdot 2^{\frac{n}{2}}-2$.

Therefore, according to Proposition 2, we have

$$\begin{aligned}&\mathrm{nl}_3(f)\\&\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n}-2c_3}+2^n}\\&=2^{n-1}-\\&\frac{1}{2}\sqrt{(2^n-1)\sqrt{3\cdot 2^{\frac{3n+1}{2}}+(5\cdot 2^{\frac{3}{2}}+2)2^n-2^{\frac{n+7}{2}}}+2^n}\\&\geq 2^{n-1}-2^{\frac{7n-7}{8}+\frac{1}{4}\log_2 3}-O(2^{\frac{3}{8}n}),\end{aligned}$$

where

$$\begin{aligned}c_3=&(2^{n-1}-2^{\frac{n+1}{2}})(2^{n-1}-5\cdot 2^{\frac{n}{2}})+\\&(2^{n-1}-2^{\frac{n+3}{2}})(2^{n-1}+5\cdot 2^{\frac{n}{2}}-2).\end{aligned}$$

For $3\mid n$, according to Corollary 2, (19) and (20), we have the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{nl}(D_{ab}D_af)\geq 2^{n-1}-2^{\frac{n+1}{2}}$ is at least $2^{n-1}-2^{\frac{n}{2}+3}$; the number of elements $b\in\mathbb{F}_{2^n}\setminus\{0,1\}$ such that $\mathrm{nl}(D_{ab}D_af)\geq 2^{n-1}-2^{\frac{n+3}{2}}$ is at most $2^{n-1}+2^{\frac{n}{2}+3}-2$.

Therefore, according to Proposition 2, we have

$$\begin{aligned}&\mathrm{nl}_3(f)\\&\geq 2^{n-1}-\frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{2n}-2c_4}+2^n}\\&=2^{n-1}-\\&\frac{1}{2}\sqrt{(2^n-1)\sqrt{3\cdot 2^{\frac{3n+1}{2}}+(2^{\frac{9}{2}}+2)\cdot 2^n-2^{\frac{n+7}{2}}}+2^n}\\&\geq 2^{n-1}-2^{\frac{7n-7}{8}+\frac{1}{4}\log_2 3}-O(2^{\frac{3}{8}n}),\end{aligned}$$

where

$$\begin{aligned}c_4=&(2^{n-1}-2^{\frac{n+1}{2}})(2^{n-1}-2^{\frac{n}{2}+3})\\&+(2^{n-1}-2^{\frac{n+3}{2}})(2^{n-1}+2^{\frac{n}{2}+3}-2).\end{aligned}$$

□

Table 8 The minimum value of $\mathrm{wt}(\mathrm{tr}_n(\lambda x^{\frac{2^n-8}{3}} + x))$ for all $\lambda \in \mathbb{F}_{2^n}^*$, odd n.

n	7	9	11	13
$\mathrm{wt}(\mathrm{tr}_n(\lambda x^{\frac{2^n-8}{3}} + x))$	≥ 56	≥ 228	≥ 976	≥ 3968
n	15	17	19	
$\mathrm{wt}(\mathrm{tr}_n(\lambda x^{\frac{2^n-8}{3}} + x))$	≥ 16064	≥ 64912	≥ 260816	

Table 9 The minimum value of $\mathrm{wt}(\mathrm{tr}_n(\lambda x^{2^n-8} + x^3))$ for all $\lambda \in \mathbb{F}_{2^n}^*$, even n.

n	8	10	12	14
$\mathrm{wt}(\mathrm{tr}_n(\lambda x^{2^n-8} + x^3))$	≥ 112	≥ 480	≥ 1944	≥ 8000
n	16	18	20	
$\mathrm{wt}(\mathrm{tr}_n(\lambda x^{2^n-8} + x^3))$	≥ 32256	≥ 129440	≥ 521664	

Table 10 Lower bounds on $\mathrm{nl}_3(\mathrm{tr}_n(x^{15}))$ for odd n.

n	7	9	11	13
lower bound	14	82	454	2183
n	15	17	19	
lower bound	9941	43949	189574	

Table 11 Lower bounds $\mathrm{nl}_3(\mathrm{tr}_n(x^{15}))$ for even n.

n	8	10	12	14
lower bound	33	194	976	4605
n	16	18	20	
lower bound	20713	90524	388018	

7.3 Comparison

For $7 \leq n \leq 20$, we determine the minimum Hamming weight of the function $\mathrm{tr}_n(\lambda x^{2^n-8} + x^3)$ for all $\lambda \in \mathbb{F}_{2^n}^*$ with the assistance of computers in Table 8 and Table 9. Note that $\mathrm{wt}(\mathrm{tr}_n(\lambda x^{2^n-8} + x^3)) = \mathrm{wt}(\mathrm{tr}_n(\lambda x^{\frac{2^n-8}{3}} + x))$ for odd n.

According to Proposition 2, Corollary 1, Corollary 2, (14), (16), (20), Table 8 and Table 9, we improve the lower bounds on the third-order nonlinearity of $\mathrm{tr}_n(x^{15})$ for $7 \leq n \leq 20$, which also improves the lower bounds on $\rho(3,n)$ for $7 \leq n \leq 20$.

8. Conclusion

We implement an algorithm to compute the high-order nonlinearities of Boolean functions using the Fourquet-Tavernier algorithm [9] and the Fourquet algorithm [10]. Among monomial Boolean functions, we find some 11-variable monomial Boolean functions with second-order nonlinearity 856 and some 8-variable monomial Boolean functions with third-order nonlinearity 56. We determine that the largest third-order nonlinearity of all non-equivalent cosets in $\mathrm{RM}(4,8)/\mathrm{RM}(3,8)$ is 56. Therefore, we prove that $\rho(2,11) \geq 856$ and the covering radius of $\mathrm{RM}(3,8)$ in $\mathrm{RM}(4,8)$ is 56. Moreover, we prove that the complexity of the Fourquet list-decoding algorithm for $\mathrm{RM}(r,n)$ can be linear in 2^n given the decoding radius close to 2^{n-r} in some special cases. Inspired by the work in [12], we improve the best proven lower bound on the third-order nonlinearity of monomial Boolean functions following from the Carlet's method.

Acknowledgments

This work was supported in part by the Innovation Action Plan of Shanghai Science and Technology under Grant 24BC3201100.

Moreover, we would like to thank Jiahua Xu for writing the code of the Fourquet algorithm.

References

[1] E. Berlekamp and L. Welch, "Weight distributions of the cosets of the (32, 6) Reed-Muller code," IEEE Trans. Inf. Theory, vol.18, no.1, pp.203–207, 1972.
[2] E. Brier and P. Langevin, "Classification of Boolean cubic forms of nine variables," Proc. - IEEE Inf. Theory Workshop, ITW (Cat. no.03EX674), pp.179–182, 2003.
[3] A. Bhowmick and S. Lovett, "The list decoding radius of Reed-Muller codes over small fields," Proc. Annu. ACM Symp. Theory Comput., pp.277–285, 2015.
[4] L. Carlitz, "Explicit evaluation of certain exponential sums," Math. Scand., vol.44, no.1, pp.5–16, 1979.
[5] A. Canteaut, P. Charpin, and G.M. Kyureghyan, "A new class of monomial bent functions," Finite Fields Their Appl., vol.14, no.1, pp.221–241, 2008.
[6] C. Carlet, "Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications," IEEE Trans. Inf. Theory, vol.54, no.3, pp.1262–1272, 2008.
[7] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, 2021.
[8] R. Dougherty, R.D. Mauldin, and M. Tiefenbruck, "The covering radius of the Reed–Muller code $RM(m-4,m)$ in $RM(m-3,m)$," IEEE Trans. Inf. Theory, vol.68, no.1, pp.560–571, 2021.
[9] R. Fourquet and C. Tavernier, "An improved list decoding algorithm for the second order Reed–Muller codes and its applications," Des. Codes Cryptogr., vol.49, pp.323–340, 2008.
[10] R. Fourquet, "List decoding of Reed-Muller codes with linear complexity up to the Johnson bound," Proc. Int. Workshop Algebr. Comb. Coding Theory, ACCT, pp.151–156, 2012.
[11] J. Gao, H. Kan, Y. Li, and Q. Wang, "The covering radius of the third-order Reed-Muller code RM(3,7) is 20," IEEE Trans. Inf. Theory, vol.69, no.6, pp.3663–3673, 2023.
[12] J. Gao, H. Kan, Y. Li, J. Xu, and Q. Wang, "Monomial Boolean functions with large high-order nonlinearities," Inf. Comput., vol.297, p.105152, 2023.
[13] V. Gillot and P. Langevin, "Classification of some cosets of the Reed-Muller code," Cryptogr. Commun., vol.15, pp.1129–1137, 2023.
[14] V. Gillot and P. Langevin, "Covering radius of $RM(4,8)$," Adv. Math. Commun., vol.18, no.2, pp.383–393, 2024.
[15] X.d. Hou, "$GL(m,2)$ acting on $R(r,m)/R(r-1,m)$," Discret. Math., vol.149, no.1-3, pp.99–122, 1996.
[16] X.d. Hou, "On the covering radius of R(1,m) in R(3,m)," IEEE Trans.

Inf. Theory, vol.42, no.3, pp.1035–1037, 1996.

[17] S. Kavut and M.D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," Inf. Comput., vol.208, no.4, pp.341–350, 2010.

[18] S. Kavut and S. Maitra, "Patterson–Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound," IEEE Trans. Inf. Theory, vol.62, no.4, pp.2277–2282, 2016.

[19] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[20] P. Langevin and G. Leander, "Classification of Boolean quartics forms in eight variables," Boolean Functions in Cryptology and Information Security, pp.139–147, IOS Press, 2008.

[21] A.M. McLoughlin, "The covering radius of the $(m-3)$rd order Reed-Muller codes and a lower bound on the $(m-4)$th order Reed-Muller codes," SIAM J. Appl. Math., vol.37, no.2, pp.419–422, 1979.

[22] J. Mykkeltveit, "The covering radius of the (128, 8) Reed-Muller code is 56 (Corresp.)," IEEE Trans. Inf. Theory, vol.26, no.3, pp.359–362, 1980.

[23] N.J. Patterson and D.H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276.," IEEE Trans. Inf. Theory, vol.29, no.3, pp.354–355, 1983.

[24] J. Schatz, "The second order Reed-Muller code of length 64 has covering radius 18 (Corresp.)," IEEE Trans. Inf. Theory, vol.27, no.4, pp.529–530, 1981.

[25] A.G. Shanbhag, P.V. Kumar, and T. Helleseth, "An upper bound for the extended Kloosterman sums over galois rings," Finite Fields Their Appl., vol.4, no.3, pp.218–238, 1998.

[26] Q. Wang, "The covering radius of the Reed–Muller code $RM(2,7)$ is 40," Discret. Math., vol.342, no.12, p.111625, 2019.

Jinjie Gao received the Ph.D. degree in computer science from Fudan University, Shanghai, China, in 2024. In 2024, she joined East China Normal University, where she is currently an associate researcher. Her research interests are cryptography, coding theory and blockchain.