Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 5(5): 4581–4595.
DOI:10.3934/math.2020294
Received: 14 January 2020
Accepted: 14 May 2020
Published: 22 May 2020

Research article

The nonlinearity and Hamming weights of rotation symmetric Boolean functions of small degree

Liping Yang, Shaofang Hong* **and Yongchao Xu**

Mathematical College, Sichuan University, Chengdu 610064, P. R. China

* **Correspondence:** Email: sfhong@scu.edu.cn; Tel: +862885412720; Fax: +862885471501.

Abstract: Let e, l and n be integers such that $1 \le e < n$ and $3 \le l \le n$. Let $\langle i \rangle$ denote the least nonnegative residue of $i \mod n$. In this paper, we investigate the following Boolean function

$$F^n_{l,e}(x^n) = \sum_{i=0}^{n-1} x_i x_{\langle i+e \rangle} x_{\langle i+2e \rangle} \dots x_{\langle i+(l-1)e \rangle},$$

which plays an important role in cryptography and coding theory. We introduce some new subfunctions and provide some recursive formulas for the Fourier transform. Using these recursive formulas, we show that the nonlinearity of $F^n_{l,e}(x^n)$ is the same as its weight for $5 \le l \le 7$. Our result confirms partially a conjecture of Yang, Wu and Hong raised in 2013. It also gives a partial answer to a conjecture of Castro, Medina and Stănică proposed in 2018. Our result extends the result of Zhang, Guo, Feng and Li for the case $l = 3$ and that of Yang, Wu and Hong for the case $l = 4$.

Keywords: Boolean function; rotation symmetric Boolean function; nonlinearity; weight; Fourier transform
Mathematics Subject Classification: Primary 06E30, 94C10

1. Introduction

Let $\mathbb{F}_2^n$ be the vector space of dimension n over the two-element field $\mathbb{F}_2 = \{0, 1\}$. A *Boolean function* $f^n(x_0, \cdots, x_{n-1})$ in n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Boolean functions have wide applications to different scientific areas, like information theory, electrical engineering, game theory, cryptography and coding theory. In 1999, Pieprzyk and Qu [8] introduced a kind of special Boolean functions such that their evaluations on every cyclic inputs are the same, which is called rotation symmetric Boolean functions (abbr. RSBFs). Further, Pieprzyk and Qu [8] showed that RSBFs are useful in the design of fast hashing algorithms with strong cryptographic properties. Since then, RSBFs have attracted much attention for their wide applications in cryptography and coding theory ([2, 5, 9]).

For brevity, let the vectors $(x_0, x_1, ..., x_{n-1})$ and $(c_0, c_1, ..., c_{n-1})$ in $\mathbb{F}_2^n$ be denoted by x^n and c^n respectively. The *Hamming weight* of a function $f^n(x^n)$ is the number of $x^n \in \mathbb{F}_2^n$ satisfying $f^n(x^n) = 1$ and denoted by $wt(f^n)$. For any two n variables Boolean functions $f^n(x^n)$ and $g^n(x^n)$, the *Hamming distance* between $f^n(x^n)$ and $g^n(x^n)$ is defined as $wt(f^n + g^n)$, and denoted by $d(f^n, g^n)$. We define the linear function L_{c^n} by $L_{c^n}(x^n) := c^n \cdot x^n$, where $\cdot$ is the vector dot product. The *nonlinearity* of f^n is defined as $N_{f^n} := \min\{d(f^n, L_{c^n}) \mid c^n \in \mathbb{F}_2^n\}$. Since hashing algorithm employing RSBFs with degree 2 as components cannot resist the linear and differential attacks [7], we need to use higher-degree RSBFs with high nonlinearity to protect from differential attack. As early as 1998, Filiol and Fontaine [4] studied the nonlinearity of RSBFs up to 9 variables. In this paper, we study the relation between Hamming weights and nonlinearity of RSBFs with small degree.

By $\langle i \rangle$ we denote the least nonnegative residue of $i \mod n$. Let e and l be integers such that $1 \leq e < n$ and $2 \leq l \leq n$. Then the *l-th rotation symmetric Boolean function* $F_{l,e}^n$ in n variables generated by the monomial $x_0 x_e x_{\langle 2e \rangle} ... x_{\langle (l-1)e \rangle}$ is defined as

$$F_{l,e}^n = F_{l,e}^n(x_0, ..., x_{n-1}) := \sum_{i=0}^{n-1} x_i x_{\langle i+e \rangle} x_{\langle i+2e \rangle} ... x_{\langle i+(l-1)e \rangle}.$$

In 2009, Kim, Park and Hahn [6] explored the nonlinearity of $F_{2,e}^n$, and proved that if $\frac{n}{\gcd(n,e)}$ is even, then $N_{F_{2,e}^n} = wt(F_{2,e}^n)$, otherwise, $N_{F_{2,e}^n} \neq wt(F_{2,e}^n)$. In 2010, Ciungu [3] showed that the linearity of $F_{3,1}^n$ is the same as its weight for the case $l = 3$ and $3|n$. Zhang, Guo, Feng and Li [11] totally proved the equality of the linearity of $F_{3,1}^n$ and its weight. Later on, Yang, Wu and Hong [10] investigated the case $l = 4$ and proved that $wt(F_{4,e}^n) = N_{F_{4,e}^n}$. Furthermore, Yang, Wu and Hong [10] proposed the following conjecture.

Conjecture 1.1. [10] Let $e \geq 1$ and $l \geq 5$ be any given integer. Then the nonlinearity of $F_{l,e}^n$ is equal to its weight.

Recently, Castro, Medina and Stănică [2] showed that the Walsh transforms of symmetric and rotation symmetric Boolean functions satisfy the linear recurrence with integer coefficients, and suggested the following conjecture:

Conjecture 1.2. [2] Let $l > 1$ be a fixed integer. The sequence of $\{N_{F_l^i}\}_{i \geq l}$ satisfies the linear recurrence whose characteristic polynomial is given by

$$x^l - 2(x^{l-2} + x^{l-2} + \cdots + x + 1) = 0.$$

In this paper, we dedicate to prove that Conjecture 1.1 is true for some small degree cases, which also confirms Conjecture 1.2 for $l = 5, 6$ and 7. Particularly, we prove the following result.

Theorem 1.3. *Let* $l \in \{5, 6, 7\}$ *and* e *and* n *be integers such that* $1 \leq e < n$ *and* $n \geq 2l - 1$. *Then* $N_{F_{l,e}^n} = wt(F_{l,e}^n)$.

This paper is organized as follows. In Section 2, we study Fourier transform of Boolean functions and obtain some recursive formulas. In Section 3, we give the proof of Theorem 1.3. The final section is devoted to some remarks.

2. Fourier transform of Boolean functions

We define the *Fourier transform* of the Boolean function $f^n(x^n)$ at $c^n \in \mathbb{F}_2^n$ to be

$$\widehat{f^n}(c^n) := \sum_{x^n \in \mathbb{F}_2^n} (-1)^{f^n(x^n)+c^n\cdot x^n}.$$

Obviously, we have $\widehat{f^n}(c^n) = 2^n - 2wt(f^n + L_{c^n})$. In particular, one has $\widehat{f^n}(0) = 2^n - 2wt(f^n)$.

First of all, we introduce some notations. We let $F_l^n := F_{l,1}^n$. Let i', j' and k' be nonnegative integers such that $1 \le k' \le j' - i' + 1$. Let m and t be nonnegative integers such that $t \le m$. Let $X(i', j', 0) := 0$, $Y(m, 0) := 0$,

$$X(i', j', k') := \sum_{r=0}^{k'-1} \prod_{s=i'+r}^{j'} x_s \text{ and } Y(m,t) := \sum_{r=1}^{t} \prod_{s=0}^{m-r} x_s.$$

Let n be an integer with $n \ge l$. Then we let

$$t_n := \sum_{s=0}^{n-l} x_s x_{s+1} \dots x_{s+l-1}.$$

For any integers i, j with $0 \le i, j \le l-1$, we let

$$f_{i,j}^n(x^n) := t_n + X(n-(l-1), n-1, i) + Y(l-1, j).$$

Now we let $n > l$. It is easy to check that if $x_{n-1} = 0$, then $t_n = t_{n-1}$ and $X(n-(l-1), n-1, i) = 0$ for any $0 \le i \le l-1$. This implies that if $x_{n-1} = 0$, then

$$t_n + X(n-(l-1), n-1, i) = t_{n-1} \tag{2.1}$$

with $0 \le i \le l-1$. If $x_{n-1} = 1$, then we derive that

$$t_n + X(n-(l-1), n-1, i) = \begin{cases} t_{n-1} + X(n-l, n-2, i+1), & \text{if } i = 0, 1, ..., l-2, \\ t_{n-1} + X(n-l, n-2, i) + 1, & \text{if } i = l-1. \end{cases} \tag{2.2}$$

Lemma 2.1. *Let l and n be integers such that $n > l \ge 5$. Let i and j be integers such that $0 \le i, j \le l-1$. If $0 \le i \le l-2$, then*

$$\widehat{f_{i,j}^n}(c^n) = \widehat{f_{0,j}^{n-1}}(c^{n-1}) + (-1)^{c_{n-1}} \widehat{f_{i+1,j}^{n-1}}(c^{n-1}).$$

If $i = l-1$, then

$$\widehat{f_{i,j}^n}(c^n) = \widehat{f_{0,j}^{n-1}}(c^{n-1}) - (-1)^{c_{n-1}} \widehat{f_{i,j}^{n-1}}(c^{n-1}).$$

Proof. We only prove the relation $\widehat{f_{l-1,0}^n}(c^n) = \widehat{f_{0,0}^{n-1}}(c^{n-1}) - (-1)^{c_{n-1}} \widehat{f_{l-1,0}^{n-1}}(c^{n-1})$. The remaining relations can be handled similarly. It follows from (2.1) and (2.2) that

$$\begin{aligned} \widehat{f_{l-1,0}^n}(c^n) &= \Big(\sum_{x^n : x_{n-1}=0} + \sum_{x^n : x_{n-1}=1} \Big) (-1)^{t_n + X(n-(l-1), n-1, l-1) + c^n \cdot x^n} \\ &= \sum_{x^{n-1}} (-1)^{t_{n-1} + c^{n-1}\cdot x^{n-1}} + \sum_{x^{n-1}} (-1)^{t_{n-1} + X(n-l, n-2, l-1) + 1 + c_{n-1} + c^{n-1}\cdot x^{n-1}} \\ &= \widehat{f_{0,0}^{n-1}}(c^{n-1}) - (-1)^{c_{n-1}} \widehat{f_{l-1,0}^{n-1}}(c^{n-1}) \end{aligned}$$

as desired. Thus Lemma 2.1 is proved. □

Let $(c_{n-l+1}, c_{n-l+2}, \ldots, c_{n-1}) \in \mathbb{F}_2^{l-1}$. If $n \geq 2l-1$, then F_l^n can be written as

$$F_l^n = t_{n-l+1} + \sum_{i=1-l}^{l-2} \prod_{j=1}^{l} x_{\langle n-l+j+i \rangle}.$$

Now we let $(x_{n-l+1}, \cdots, x_{n-1})$ take all values in $\mathbb{F}_2^{l-1}$. If $l = 5$, then

$$\begin{aligned}
\widehat{F_5^n}(c^n) = & \prod_{s=2}^{3}(1+(-1)^{c_{n-s}})\widehat{f_{0,0}^{n-4}}(c^{n-4}) + (-1)^{c_{n-1}}(1+(-1)^{c_{n-3}})\widehat{f_{0,1}^{n-4}}(c^{n-4}) \\
& + (-1)^{c_{n-4}}(1+(-1)^{c_{n-2}})\widehat{f_{1,0}^{n-4}}(c^{n-4}) + \prod_{s=1}^{2}(-1)^{c_{n-s}}\widehat{f_{0,2}^{n-4}}(c^{n-4}) \\
& + (-1)^{c_{n-4}}\prod_{s=1}^{2}(-1)^{c_{n-s}}\widehat{f_{1,2}^{n-4}}(c^{n-4}) + (-1)^{c_{n-4}+c_{n-1}}\widehat{f_{1,1}^{n-4}}(c^{n-4}) \\
& + \prod_{s=1}^{3}(-1)^{c_{n-s}}\widehat{f_{0,3}^{n-4}}(c^{n-4}) + \prod_{s=1}^{2}(-1)^{c_{n-(5-s)}}\widehat{f_{2,0}^{n-4}}(c^{n-4}) \\
& + \prod_{s=1}^{2}(-1)^{c_{n-(5-s)}} \cdot (-1)^{c_{n-1}}\widehat{f_{2,1}^{n-4}}(c^{n-4}) + \prod_{s=1}^{3}(-1)^{c_{n-(5-s)}}\widehat{f_{3,0}^{n-4}}(c^{n-4}) + \prod_{s=1}^{4}(-1)^{c_{n-s}}\widehat{f_{4,4}^{n-4}}(c^{n-4}).
\end{aligned}$$

If $l \geq 6$, then $\widehat{F_l^n}(c^n)$ can be decomposed as follows:

$$\begin{aligned}
\widehat{F_l^n}(c^n) = & \prod_{s=2}^{l-2}(1+(-1)^{c_{n-s}})\widehat{f_{0,0}^{n-(l-1)}}(c^{n-(l-1)}) + \sum_{j=1}^{l-4}\prod_{t=1}^{j}(-1)^{c_{n-t}}\prod_{s=j+2}^{l-2}(1+(-1)^{c_{n-s}})\widehat{f_{0,j}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \sum_{i=1}^{l-4}\prod_{t=1}^{i}(-1)^{c_{n-(l-t)}}\prod_{s=2}^{l-i-2}(1+(-1)^{c_{n-s}})\widehat{f_{i,0}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \sum_{i=1}^{l-4}\sum_{j=1}^{j+i\leq l-4}\prod_{t_1=1}^{i}(-1)^{c_{n-(l-t_1)}}\prod_{t_2=1}^{j}(-1)^{c_{n-t_2}}\prod_{s=j+2}^{l-i-2}(1+(-1)^{c_{n-s}})\widehat{f_{i,j}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \prod_{t=1}^{l-3}(-1)^{c_{n-t}}\widehat{f_{0,l-3}^{n-(l-1)}}(c^{n-(l-1)}) + (-1)^{c_{n-(l-1)}}\prod_{t=1}^{l-3}(-1)^{c_{n-t}}\widehat{f_{1,l-3}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \sum_{i=2}^{l-4}\sum_{j=l-3-i}^{l-2-i}\prod_{t_1=1}^{i}(-1)^{c_{n-(l-t_1)}}\prod_{t_2=1}^{j}(-1)^{c_{n-t_2}}\widehat{f_{i,j}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + (-1)^{c_{n-(l-1)}}\prod_{t=1}^{l-4}(-1)^{c_{n-t}}\widehat{f_{1,l-4}^{n-(l-1)}}(c^{n-(l-1)}) + \prod_{t=1}^{l-2}(-1)^{c_{n-t}}\widehat{f_{0,l-2}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \prod_{t=1}^{l-3}(-1)^{c_{n-(l-t)}}\widehat{f_{l-3,0}^{n-(l-1)}}(c^{n-(l-1)}) + \prod_{t=1}^{l-3}(-1)^{c_{n-(l-t)}}(-1)^{c_{n-1}}\widehat{f_{l-3,1}^{n-(l-1)}}(c^{n-(l-1)}) \\
& + \prod_{t=1}^{l-2}(-1)^{c_{n-(l-t)}}\widehat{f_{l-2,0}^{n-(l-1)}}(c^{n-(l-1)}) + \prod_{t=1}^{l-1}(-1)^{c_{n-t}}\widehat{f_{l-1,l-1}^{n-(l-1)}}(c^{n-(l-1)}).
\end{aligned} \tag{2.3}$$

Now we let $c^n = (0, \cdots, 0)$. Clearly, we have $f^n_{i,j}(x_0, ..., x_{n-1}) = f^n_{j,i}(x_{n-1}, ..., x_0)$. Hence $\widehat{f^n_{i,j}}(0) = \widehat{f^n_{j,i}}(0)$. Thus we conclude that if $l = 5$, then

$$\widehat{F^n_5}(0) = 4\widehat{f^{n-4}_{0,0}}(0) + 4\widehat{f^{n-4}_{0,1}}(0) + 2\widehat{f^{n-4}_{0,2}}(0) + 2\widehat{f^{n-4}_{1,2}}(0) + \widehat{f^{n-4}_{1,1}}(0) + 2\widehat{f^{n-4}_{0,3}}(0) + \widehat{f^{n-4}_{4,4}}(0).$$

And if $l \geq 6$, then

$$\begin{aligned}\widehat{F^n_l}(0) = &\sum_{i=0}^{l-4} \sum_{j=0}^{j+i \leq l-4} 2^{l-3-i-j} \widehat{f^{n-(l-1)}_{i,j}}(0) + \widehat{f^{n-(l-1)}_{1,l-4}}(0) + 2\widehat{f^{n-(l-1)}_{0,l-2}}(0) \\ &+ \sum_{i=2}^{l-4} \sum_{j=l-3-i}^{l-2-i} \widehat{f^{n-(l-1)}_{i,j}}(0) + 2\sum_{i=0}^{1} \widehat{f^{n-(l-1)}_{i,l-3}}(0) + \widehat{f^{n-(l-1)}_{l-1,l-1}}(0). \end{aligned} \tag{2.4}$$

Let $[x]$ denote the largest integer that is less than or equal to the real number x. In what follows, we give some recursive relations about $\widehat{f^n_{i,j}}(c^n)$ for any integer i and j with $0 \leq i, j \leq l-1$.

Lemma 2.2. *Let n, l, i, j and k be integers such that $l \geq 5$, $n \geq 2l$, $0 \leq i, j \leq l-1$ and $1 \leq k \leq n$. Let $c^n = (c_0, ..., c_{n-1}) \in \mathbb{F}_2^n$ such that $c_{n-1} = 0$. Let c^k be the vector consisting of the first k bits of c^n. If $i = l-1$, then*

$$\widehat{f^n_{i,j}}(c^n) = \begin{cases} 2\sum\limits_{s=1}^{\frac{l-2}{2}} \prod\limits_{t=2}^{2s} (-1)^{c_{n-t}} \widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod\limits_{t=2}^{l} (-1)^{c_{n-t}} \widehat{f^{n-l}_{l-1,j}}(c^{n-l}), \textit{if i is odd}, \\ 2\sum\limits_{s=1}^{[\frac{l-2}{2}]} \prod\limits_{t=2}^{2s} (-1)^{c_{n-t}} \widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod\limits_{t=2}^{l-1} (-1)^{c_{n-t}} \widehat{f^{n-l}_{0,j}}(c^{n-l}), \textit{if i is even}. \end{cases}$$

If $i = l-2$, then

$$\widehat{f^n_{i,j}}(c^n) = \begin{cases} 2\sum\limits_{s=1}^{\frac{l-1}{2}} \prod\limits_{t=2}^{2s} (-1)^{c_{n-t}} \widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod\limits_{t=2}^{l} (-1)^{c_{n-t}} \widehat{f^{n-l}_{l-1,j}}(c^{n-l}), \textit{if i is odd}, \\ 2\sum\limits_{s=1}^{[\frac{l-1}{2}]} \prod\limits_{t=2}^{2s} (-1)^{c_{n-t}} \widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod\limits_{t=2}^{l-1} (-1)^{c_{n-t}} \widehat{f^{n-l}_{0,j}}(c^{n-l}), \textit{if i is even}. \end{cases}$$

If $0 \leq i \leq l-3$, then

$$\widehat{f^n_{i,j}}(c^n) = \begin{cases} 2\sum\limits_{s=1}^{l-2} \prod\limits_{t=1}^{s} (-1)^{c_{n-t}} \widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod\limits_{t=2}^{l-1} (-1)^{c_{n-t}} \widehat{f^{n-l}_{0,j}}(c^{n-l}), \quad \textit{if } i = 0, \\ 2\sum\limits_{s=1}^{l-3} \prod\limits_{t=1}^{s} (-1)^{c_{n-t}} \widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod\limits_{t=2}^{l-2} (-1)^{c_{n-t}} \widehat{f^{n-(l-1)}_{0,j}}(c^{n-(l-1)}) \\ +2\prod\limits_{t=2}^{l} (-1)^{c_{n-t}} \widehat{f^{n-l}_{l-1,j}}(c^{n-l}), \qquad \textit{if } i = 1, \\ 2\sum\limits_{s=1}^{l-i-2} \prod\limits_{t=1}^{s} (-1)^{c_{n-t}} \widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod\limits_{t=2}^{l-1-i} (-1)^{c_{n-t}} \Big(\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)}) \\ + \sum\limits_{s=1}^{[\frac{i}{2}]} \prod\limits_{k=0}^{2s-1} (-1)^{c_{n-(l-i+k)}} \widehat{f^{n-(l-i+2s)}_{0,j}}(c^{n-(l-i+2s)}) + \prod\limits_{k=0}^{i} (-1)^{c_{n-(l-i+k)}} \widehat{f^{n-l}_{l-1,j}}(c^{n-l})\Big), \\ \qquad \textit{if } i \geq 2 \textit{ is odd}, \\ 2\sum\limits_{s=1}^{l-i-2} \prod\limits_{t=1}^{s} (-1)^{c_{n-t}} \widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod\limits_{t=2}^{l-1-i} (-1)^{c_{n-t}} \Big(\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)}) \\ + \sum\limits_{s=1}^{\frac{i}{2}} \prod\limits_{k=0}^{2s-1} (-1)^{c_{n-(l-i+k)}} \widehat{f^{n-(l-i+2s)}_{0,j}}(c^{n-(l-i+2s)})\Big), \qquad \textit{if } i \geq 2 \textit{ is even}. \end{cases}$$

Proof. Note that $c_{n-1} = 0$. We divide the proof into the following three cases.

Case 1. $i = l - 1$. For any integer j with $0 \le j \le l-1$, by Lemma 2.1 we conclude that

$$\begin{aligned}\widehat{f^{n}_{l-1,j}}(c^{n}) =& \widehat{f^{n-1}_{0,j}}(c^{n-1}) + (-1)^{1+c_{n-1}}\widehat{f^{n-1}_{l-1,j}}(c^{n-1}) \\ =& \widehat{f^{n-2}_{0,j}}(c^{n-2}) + (-1)^{c_{n-2}}\widehat{f^{n-2}_{1,j}}(c^{n-2}) - \Big(\widehat{f^{n-2}_{0,j}}(c^{n-2}) + (-1)^{1+c_{n-2}}\widehat{f^{n-2}_{l-1,j}}(c^{n-2})\Big) \\ =& 2(-1)^{c_{n-2}}\widehat{f^{n-3}_{0,j}}(c^{n-3}) + (-1)^{c_{n-2}+c_{n-3}}\Big(\widehat{f^{n-3}_{2,j}}(c^{n-3}) + (-1)^{3}\widehat{f^{n-3}_{l-1,j}}(c^{n-3})\Big) \\ =& \cdots\cdots \\ =& 2\sum_{s=1}^{[\frac{l-2}{2}]}\prod_{t=2}^{2s}(-1)^{c_{n-t}}\widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + \prod_{t=2}^{l-1}(-1)^{c_{n-t}}\Big(\widehat{f^{n-l+1}_{l-2,j}}(c^{n-l+1}) + (-1)^{l-1}\widehat{f^{n-l+1}_{l-1,j}}(c^{n-l+1})\Big).\end{aligned}$$

If l is even, then by Lemma 2.1 one derives that

$$\widehat{f^{n}_{l-1,j}}(c^{n}) = 2\sum_{s=1}^{\frac{l-2}{2}}\prod_{t=2}^{2s}(-1)^{c_{n-t}}\widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod_{t=2}^{l}(-1)^{c_{n-t}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).$$

If l is odd, it then follows from Lemma 2.1 that

$$\widehat{f^{n}_{l-1,j}}(c^{n}) = 2\sum_{s=1}^{[\frac{l-2}{2}]}\prod_{t=2}^{2s}(-1)^{c_{n-t}}\widehat{f^{n-(2s+1)}_{0,j}}(c^{n-(2s+1)}) + 2\prod_{t=2}^{l-1}(-1)^{c_{n-t}}\widehat{f^{n-l}_{0,j}}(c^{n-l}).$$

This finishes the proof of Lemma 2.2 in this case.

Case 2. $i = l - 2$. Then by Lemma 2.1, we have

$$\begin{aligned}\widehat{f^{n}_{l-2,j}}(c^{n}) =& \widehat{f^{n-1}_{0,j}}(c^{n-1}) + \widehat{f^{n-1}_{l-1,j}}(c^{n-1}) \\ =& 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + (-1)^{c_{n-2}}\widehat{f^{n-2}_{1,j}}(c^{n-2}) + (-1)^{1+c_{n-2}}\widehat{f^{n-2}_{l-1,j}}(c^{n-2}) \\ =& 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + (-1)^{c_{n-2}+c_{n-3}}\Big(\widehat{f^{n-3}_{2,j}}(c^{n-3}) + (-1)^{2}\widehat{f^{n-3}_{l-1,j}}(c^{n-3})\Big) \\ =& \cdots\cdots \\ =& 2\sum_{s=1}^{[\frac{l-1}{2}]}\prod_{t=1}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s}) + \prod_{t=2}^{l-1}(-1)^{c_{n-t}}\Big(\widehat{f^{n-l+1}_{l-2,j}}(c^{n-l+1}) + (-1)^{l-2}\widehat{f^{n-l+1}_{l-1,j}}(c^{n-l+1})\Big).\end{aligned}$$

If l is even, then one derives that

$$\widehat{f^{n}_{l-2,j}}(c^{n}) = 2\sum_{s=1}^{[\frac{l-1}{2}]}\prod_{t=1}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s}) + 2\prod_{t=2}^{l-1}(-1)^{c_{n-t}}\widehat{f^{n-l}_{0,j}}(c^{n-l}).$$

If l is odd, then

$$\widehat{f^{n}_{l-2,j}}(c^{n}) = 2\sum_{s=1}^{\frac{l-1}{2}}\prod_{t=1}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s}) + 2\prod_{t=2}^{l}(-1)^{c_{n-t}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).$$

Thus Lemma 2.2 is proved in this case.

CASE 3. $0 \le i \le l-3$. Then by Lemma 2.1, we have

$$\begin{aligned}\widehat{f^{n}_{i,j}}(c^{n}) =&\widehat{f^{n-1}_{0,j}}(c^{n-1}) + (-1)^{c_{n-1}}\widehat{f^{n-1}_{i+1,j}}(c^{n-1})\\ =&\cdots\cdots\\ =&2\sum_{s=1}^{l-i-2}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + \prod_{t=2}^{l-1-i}(-1)^{c_{n-t}}\Big(\widehat{f^{n-(l-i-1)}_{l-i-2,j}}(c^{n-(l-i-1)}) + \widehat{f^{n-(l-i-1)}_{l-1,j}}(c^{n-(l-i-1)})\Big)\\ :=&2\sum_{s=1}^{l-i-2}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + \prod_{t=2}^{l-1-i}(-1)^{c_{n-t}}T_{n-(l-i-1)}.\end{aligned} \tag{2.5}$$

Note that $0 \le i \le l-3$. From Lemma 2.1 we derive that

$$T_{n-(l-i-1)} = 2\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)}) + (-1)^{c_{n-(l-i)}}\Big(\widehat{f^{n-(l-i)}_{l-i-1,j}}(c^{n-(l-i)}) - \widehat{f^{n-(l-i)}_{l-1,j}}(c^{n-(l-i)})\Big). \tag{2.6}$$

If $i = 0$, then it is easy to see that $T_{n-(l-1)} = 2\widehat{f^{n-l}_{0,j}}(c^{n-l})$. It follows from (2.5) that

$$\widehat{f^{n}_{0,j}}(c^{n}) = 2\sum_{s=1}^{l-2}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod_{t=2}^{l-1}(-1)^{c_{n-t}}\widehat{f^{n-l}_{0,j}}(c^{n-l}).$$

If $i = 1$, then by (2.6) and Lemma 2.1, we have

$$T_{n-(l-i-1)} = 2\widehat{f^{n-(l-1)}_{0,j}}(c^{n-(l-1)}) + 2(-1)^{c_{n-(l-1)}+c_{n-l}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).$$

Thus from (2.5), we obtain that

$$\widehat{f^{n}_{1,j}}(c^{n}) =2\sum_{s=1}^{l-3}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod_{t=2}^{l-2}(-1)^{c_{n-t}}\widehat{f^{n-(l-1)}_{0,j}}(c^{n-(l-1)}) + 2\prod_{t=2}^{l}(-1)^{c_{n-t}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).$$

If $2 \le i \le l-3$, then by (2.6) and Lemma 2.1, we have

$$\begin{aligned}T_{n-(l-i-1)} =&2\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)}) + 2\sum_{s=1}^{[\frac{i}{2}]}\prod_{k=0}^{2s-1}(-1)^{c_{n-(l-i+k)}}\widehat{f^{n-(l-i+2s)}_{0,j}}(c^{n-(l-i+2s)})\\ &+\prod_{k=0}^{i}(-1)^{c_{n-(l-i+k)}}(1+(-1)^{i+1})\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).\end{aligned}$$

Hence we obtain that if i is odd, then

$$T_{n-(l-i-1)} =2\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)}) + 2\sum_{s=1}^{[\frac{i}{2}]}\prod_{k=0}^{2s-1}(-1)^{c_{n-(l-i+k)}}\widehat{f^{n-(l-i+2s)}_{0,j}}(c^{n-(l-i+2s)}) + 2\prod_{k=0}^{i}(-1)^{c_{n-(l-i+k)}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l}).$$

By (2.5), one deduces that

$$\widehat{f^{n}_{i,j}}(c^{n}) =2\sum_{s=1}^{l-i-2}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f^{n-(s+1)}_{0,j}}(c^{n-(s+1)}) + 2\prod_{t=2}^{l-1-i}(-1)^{c_{n-t}}\Big(\widehat{f^{n-(l-i)}_{0,j}}(c^{n-(l-i)})$$

$$+\sum_{s=1}^{[\frac{i}{2}]}\prod_{k=0}^{2s-1}(-1)^{c_{n-(l-i+k)}}\widehat{f_{0,j}^{n-(l-i+2s)}}(c^{n-(l-i+2s)})+\prod_{k=0}^{i}(-1)^{c_{n-(l-i+k)}}\widehat{f_{l-1,j}^{n-l}}(c^{n-l})\Big).$$

If i is even, then

$$T_{n-(l-i-1)}=2\widehat{f_{0,j}^{n-(l-i)}}(c^{n-(l-i)})+2\sum_{s=1}^{\frac{i}{2}}\prod_{k=0}^{2s-1}(-1)^{c_{n-(l-i+k)}}\widehat{f_{0,j}^{n-(l-i+2s)}}(c^{n-(l-i+2s)}).$$

From (2.5) we derive that

$$\begin{aligned}\widehat{f_{i,j}^{n}}(c^n)=&2\sum_{s=1}^{l-i-2}\prod_{t=1}^{s}(-1)^{c_{n-t}}\widehat{f_{0,j}^{n-(s+1)}}(c^{n-(s+1)})+2\prod_{t=2}^{l-1-i}(-1)^{c_{n-t}}\Big(\widehat{f_{0,j}^{n-(l-i)}}(c^{n-(l-i)})\\&+\sum_{s=1}^{\frac{i}{2}}\prod_{k=0}^{2s-1}(-1)^{c_{n-(l-i+k)}}\widehat{f_{0,j}^{n-(l-i+2s)}}(c^{n-(l-i+2s)})\Big).\end{aligned}$$

Hence Lemma 2.2 holds in this case.

This completes the proof of Lemma 2.2. □

Lemma 2.3. *Let n, l, i, j and k be integers such that $l \geq 5$, $n \geq 2l$, $0 \leq i, j \leq l-1$ and $1 \leq k \leq n$. Let $c^n = (c_0, ..., c_{n-1}) \in \mathbb{F}_2^n$ such that $c_{n-1} = 1$. Let c^k denote the first k bits of c^n. Then*

$$\widehat{f_{i,j}^{n}}(c^n)=\begin{cases}(-1)^{c_{n-2}}\widehat{f_{1,j}^{n-2}}(c^{n-2})+(-1)^{1+c_{n-2}}\widehat{f_{i+2,j}^{n-2}}(c^{n-2}), & \textit{if } 0\leq i\leq l-3,\\ (-1)^{c_{n-2}}\widehat{f_{1,j}^{n-2}}(c^{n-2})+(-1)^{c_{n-2}}\widehat{f_{l-1,j}^{n-2}}(c^{n-2}), & \textit{if } i=l-2,\\ 2\widehat{f_{0,j}^{n-2}}(c^{n-2})+2\sum\limits_{s=2}^{[\frac{l-1}{2}]}\prod\limits_{t=2}^{2s-1}(-1)^{c_{n-t}}\widehat{f_{0,j}^{n-2s}}(c^{n-2s})+2\prod\limits_{t=2}^{l-1}(-1)^{c_{n-t}}\widehat{f_{0,j}^{n-l}}(c^{n-l}), & \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\textit{if } i=l-1 \textit{ is odd}, & \\ 2\widehat{f_{0,j}^{n-2}}(c^{n-2})+2\sum\limits_{s=2}^{\frac{l-1}{2}}\prod\limits_{t=2}^{2s-1}(-1)^{c_{n-t}}\widehat{f_{0,j}^{n-2s}}(c^{n-2s})+2\prod\limits_{t=2}^{l}(-1)^{c_{n-t}}\widehat{f_{l-1,j}^{n-l}}(c^{n-l}), & \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\textit{if } i=l-1 \textit{ is even}. & \end{cases}$$

Proof. We divide the proof into the following three cases.

Case 1. $0 \leq i \leq l-3$. Then by Lemma 2.1 we have

$$\begin{aligned}\widehat{f_{i,j}^{n}}(c^n)&=\widehat{f_{0,j}^{n-1}}(c^{n-1})-\widehat{f_{i+1,j}^{n-1}}(c^{n-1})\\&=\widehat{f_{0,j}^{n-2}}(c^{n-2})+(-1)^{c_{n-2}}\widehat{f_{1,j}^{n-2}}(c^{n-2})-\widehat{f_{0,j}^{n-2}}(c^{n-2})-(-1)^{c_{n-2}}\widehat{f_{i+2,j}^{n-2}}(c^{n-2})\\&=(-1)^{c_{n-2}}\widehat{f_{1,j}^{n-2}}(c^{n-2})+(-1)^{1+c_{n-2}}\widehat{f_{i+2,j}^{n-2}}(c^{n-2}).\end{aligned}$$

Thus Lemma 2.3 is true in this case.

Case 2. $i = l-2$. From Lemma 2.1 one deduces that

$$\begin{aligned}\widehat{f_{l-2,j}^{n}}(c^n)&=\widehat{f_{0,j}^{n-1}}(c^{n-1})-\widehat{f_{l-1,j}^{n-1}}(c^{n-1})\\&=\widehat{f_{0,j}^{n-2}}(c^{n-2})+(-1)^{c_{n-2}}\widehat{f_{1,j}^{n-2}}(c^{n-2})-\widehat{f_{0,j}^{n-2}}(c^{n-2})+(-1)^{2+c_{n-2}}\widehat{f_{l-1,j}^{n-2}}(c^{n-2})\end{aligned}$$

$$= (-1)^{c_{n-2}}\widehat{f^{n-2}_{1,j}}(c^{n-2}) + (-1)^{c_{n-2}}\widehat{f^{n-2}_{l-1,j}}(c^{n-2}).$$

Hence Lemma 2.3 holds for this case.

Case 3. $i = l - 1$. It follows from Lemma 2.1 that

$$\begin{aligned}\widehat{f^{n}_{l-1,j}}(c^{n}) &= \widehat{f^{n-1}_{0,j}}(c^{n-1}) - (-1)^{c_{n-1}}\widehat{f^{n-1}_{l-1,j}}(c^{n-1})\\ &= 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + (-1)^{c_{n-2}}\Big(\widehat{f^{n-2}_{1,0}}(c^{n-2}) - \widehat{f^{n-2}_{l-1,j}}(c^{n-2})\Big)\\ &= \cdots\cdots\\ &= 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + 2\sum_{s=2}^{[\frac{l-1}{2}]}\prod_{t=2}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s})\\ &\quad + \prod_{t=2}^{l-1}(-1)^{c_{n-t}}\Big(\widehat{f^{n-l+1}_{l-2,j}}(c^{n-l+1}) + (-1)^{l-2}\widehat{f^{n-l+1}_{l-1,j}}(c^{n-l+1})\Big).\end{aligned}$$

If l is even, then one derives that

$$\widehat{f^{n}_{l-1,j}}(c^{n}) = 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + 2\sum_{s=2}^{[\frac{l-1}{2}]}\prod_{t=2}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s}) + 2\prod_{t=2}^{l-1}(-1)^{c_{n-t}}\widehat{f^{n-l}_{0,j}}(c^{n-l})$$

as desired.

If l is odd, then

$$\widehat{f^{n}_{l-1,j}}(c^{n}) = 2\widehat{f^{n-2}_{0,j}}(c^{n-2}) + 2\sum_{s=2}^{\frac{l-1}{2}}\prod_{t=2}^{2s-1}(-1)^{c_{n-t}}\widehat{f^{n-2s}_{0,j}}(c^{n-2s}) + 2\prod_{t=2}^{l}(-1)^{c_{n-t}}\widehat{f^{n-l}_{l-1,j}}(c^{n-l})$$

as required. Hence Lemma 2.3 is proved in this case.

This finishes the proof of Lemma 2.3. □

Lemma 2.4. *Let l, n, j be integers such that $l \geq 5$, $n \geq 2l$ and $0 \leq j \leq l-1$. Then for integer i with $0 \leq i \leq l-1$, we have*

$$\widehat{f^{n}_{i,j}}(0) = 2\sum_{s=2}^{l}\widehat{f^{n-s}_{i,j}}(0). \tag{2.7}$$

Proof. It follows from Lemma 2.2 that for any integer j with $0 \leq j \leq l-1$, we have

$$\widehat{f^{n}_{0,j}}(0) = 2\sum_{s=2}^{l}\widehat{f^{n-s}_{0,j}}(0).$$

Thus (2.7) is true when $i = 0$ and $0 \leq j \leq l-1$. Note that $\widehat{f^{n}_{i,j}}(0) = \widehat{f^{n}_{j,i}}(0)$. Then for $0 \leq i \leq l-1$, one has

$$\widehat{f^{n}_{i,0}}(0) = 2\sum_{s=2}^{l}\widehat{f^{n-s}_{i,0}}(0).$$

Then by the definition of $\widehat{f^{n}_{i,j}}(0)$ and the assumption $n \geq 2l-1$, we can conclude that (2.7) holds for any integer $0 \leq i, j \leq l-1$. Hence Lemma 2.4 is proved. □

In the following, we show that the weight of F_l^n satisfies a linear recurrence, which is also proved by Castro, Chapman, Medina and Sepúlveda [1].

Proposition 2.5. *Let l and n be integers such that $l \geq 5$ and $n \geq 2l$. Then*

$$\widehat{F_l^n}(0) = 2\sum_{s=2}^{l}\widehat{F_l^{n-s}}(0).$$

Proof. We only prove the case $l \geq 6$ since the case $l = 5$ can be done similarly. Let $l \geq 6$. It then follows from (2.4) and Lemma 2.4 that

$$\begin{aligned}\widehat{F_l^n}(0) =& 2\sum_{i=0}^{l-4}\sum_{j=0}^{j+i\leq l-4} 2^{l-3-i-j}\sum_{s=2}^{l}\widehat{f_{i,j}^{n-l+1-s}}(0) + 2\sum_{s=2}^{l}\widehat{f_{1,l-4}^{n-l+1-s}}(0) + 4\sum_{i=0}^{1}\sum_{s=2}^{l}\widehat{f_{i,l-3}^{n-l+1-s}}(0)\\ &+ 2\sum_{i=2}^{l-4}\sum_{j=l-3-i}^{l-2-i}\sum_{s=2}^{l}\widehat{f_{i,j}^{n-l+1-s}}(0) + 4\sum_{s=2}^{l}\widehat{f_{0,l-2}^{n-l+1-s}}(0) + 2\sum_{s=2}^{l}\widehat{f_{l-1,l-1}^{n-l+1-s}}(0).\end{aligned}$$

Then by (2.4), we deduce that

$$\begin{aligned}\widehat{F_l^n}(0) =& 2\sum_{s=2}^{l}\Big(\sum_{i=0}^{l-4}\sum_{j=0}^{j+i\leq l-4} 2^{l-3-i-j}\widehat{f_{i,j}^{n-l+1-s}}(0) + \widehat{f_{1,l-4}^{n-l+1-s}}(0) + \sum_{i=0}^{1} 2\widehat{f_{i,l-3}^{n-l+1-s}}(0)\\ &+ \sum_{i=2}^{l-4}\sum_{j=l-3-i}^{l-2-i}\widehat{f_{i,j}^{n-l+1-s}}(0) + 2\widehat{f_{0,l-2}^{n-l+1-s}}(0) + \widehat{f_{l-1,l-1}^{n-l+1-s}}(0)\Big)\\ =& 2\sum_{s=2}^{l}\widehat{F_l^{n-s}}(0).\end{aligned}$$

The proof of Proposition 2.5 is complete. □

Lemma 2.6 (Proposition 3.1, [10])**.** *Let $f^n(x^n)$ be a Boolean function with n variables. If $\widehat{f^n}(0) = \max\{|\widehat{f^n}(c^n)| : c^n \in \mathbb{F}_2^n\}$, then $N_{f^n} = wt(f^n)$.*

3. Proof of Theorem 1.3

In this section, we show Theorem 1.3. For this purpose, we need the following lemma.

Lemma 3.1. *Let n and l be nonnegative integers such that $5 \leq l \leq 7$. Let $c^n = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n$. If c^n such that $c_1 = 1$, then for all $0 \leq i, j \leq l-1$, we have*

$$|\widehat{f_{i,j}^n}(c^n)| < \frac{1}{2^{l-1}}\widehat{F_l^{n+l-1}}(0). \tag{3.1}$$

Proof. We prove Lemma 3.1 by induction on n. When $l \leq n \leq 2l-1$ and $c_1 \neq 0$, using Maple 17 we can check that (3.1) holds for all $0 \leq i, j \leq l-1$. For example, the case $l = n = 5$ is given in Table 1, we can check that $\widehat{f_{ij}^n}(c^5) \leq \frac{1}{2^4}\widehat{F_l^{2l-1}}(0) = \frac{420}{2^4}$. In what follows, we let $n \geq 2l$. Assume that Lemma 3.1 holds for any positive integer k less than $n-1$. Now we prove that Lemma 3.1 is true for the case $k = n$. Since $c_1 = 1$, we divide the proof into the following two cases.

Table 1. The evaluations of $\widehat{f^5_{i,j}}(c^5)$, $0 \le i, j \le 4$, where $c^5 = (c_0, ...c_4) \in \mathbb{F}_2^5$ with $c_1 \neq 0$ is denoted by $\sum_{0\le i\le 4} c_i 2^i$.

c	2	3	6	7	10	11	14	15	18	19	22	23	26	27	30	31
$\widehat{f^5_{0,0}}$	2	-2	-2	2	-2	2	2	-2	-2	2	2	-2	2	-2	-2	2
$\widehat{f^5_{0,1}}$	2	-2	-2	2	-2	2	2	-2	2	-2	-2	2	-2	2	2	-2
$\widehat{f^5_{0,2}}$	6	-6	-6	6	2	-2	-2	2	-2	2	2	-2	2	-2	-2	2
$\widehat{f^5_{0,3}}$	10	-10	6	-6	-2	2	2	-2	2	-2	-2	2	-2	2	2	-2
$\widehat{f^5_{0,4}}$	-10	10	-6	6	2	-2	-2	2	-2	2	2	-2	2	-2	-2	2
$\widehat{f^5_{1,0}}$	2	2	-2	-2	-2	-2	2	2	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{1,1}}$	6	-2	-6	2	-6	2	6	-2	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{1,2}}$	6	-2	-6	2	2	-6	-2	6	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{1,3}}$	14	-10	2	-6	-6	2	6	-2	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{1,4}}$	-10	14	-6	2	2	-6	-2	6	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{2,0}}$	-2	-2	2	2	2	2	-2	-2	2	2	-2	-2	-2	-2	2	2
$\widehat{f^5_{2,1}}$	-2	-2	2	2	2	2	-2	-2	6	-2	-6	2	-6	2	6	-2
$\widehat{f^5_{2,2}}$	2	-6	-2	6	6	-2	-6	2	2	2	-2	-2	-2	-2	2	2
$\widehat{f^5_{2,3}}$	6	-10	-6	10	10	-6	-10	6	2	2	-2	-2	-2	-2	2	2
$\widehat{f^5_{2,4}}$	-10	6	-6	10	2	2	-2	-2	-2	6	2	-6	2	-6	-2	6
$\widehat{f^5_{3,0}}$	2	2	-2	-2	-2	-2	2	2	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{3,1}}$	6	-2	-6	2	-6	2	6	-2	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{3,2}}$	6	-2	-6	2	2	-6	-2	6	-2	-2	2	2	2	2	-2	-2
$\widehat{f^5_{3,3}}$	10	-6	-2	-2	-2	-2	10	-6	2	-6	6	-2	-2	6	-6	2
$\widehat{f^5_{3,4}}$	-6	10	-2	-2	-2	-2	-6	10	-6	2	-2	6	6	-2	2	-6
$\widehat{f^5_{4,0}}$	-2	-2	2	2	2	2	-2	-2	2	2	-2	-2	-2	-2	2	2
$\widehat{f^5_{4,1}}$	-2	-2	2	2	2	2	-2	-2	6	-2	-6	2	-6	2	6	-2
$\widehat{f^5_{4,2}}$	-2	-2	2	2	2	2	-2	-2	6	-2	-6	2	2	-6	-2	6
$\widehat{f^5_{4,3}}$	2	-6	6	-2	-2	6	-6	2	10	-6	-2	-2	-2	-2	10	-6
$\widehat{f^5_{4,4}}$	-6	2	-2	6	6	-2	2	-6	-6	10	-2	-2	-2	-2	-6	10

Case 1. $c_{n-1} = 0$. From Lemma 2.2 and Theorem 2.5, then

$$|\widehat{f^n_{i,j}}(c^n)| < \frac{2}{2^{l-1}}\Big(\widehat{F_l^{n-2+l-1}}(0) + \widehat{F_l^{n-3+l-1}}(0) + \cdots + \widehat{F_l^{n-l+l-1}}(0)\Big) = \frac{1}{2^{l-1}}\widehat{F_l^{n+l-1}}(0).$$

Hence Lemma 3.1 is true in this case.

Case 2. $c_{n-1} = 1$. Then by Lemma 2.3 and Theorem 2.5 we have

$$|\widehat{f^n_{i,j}}(c^n)| <\frac{2}{2^{l-1}}\Big(\widehat{F_l^{n-2+l-1}}(0) + \widehat{F_l^{n-3+l-1}}(0) + \cdots + \widehat{F_l^{n-l+l-1}}(0)\Big) = \frac{1}{2^{l-1}}\widehat{F_l^{n+l-1}}(0).$$

Thus Lemma 3.1 holds for this case.

This finishes the proof of Lemma 3.1. □

Now we present the proof of Theorem 1.3.

Proof of Theorem 1.3. From Lemma 2.6 we conclude that to prove the validity of Theorem 1.3 for $e = 1$, it suffices to prove that

$$\widehat{F^n_l}(0) = \max\{|\widehat{F^n_l}(c^n)| : c^n \in \mathbb{F}_2^n\}.$$

From the definition of F^n_l, we conclude that for any integer $0 \le j \le n-1$,

$$\widehat{F^n_l}(c_0, c_1, \cdots, c_{n-1}) = \widehat{F^n_l}(c_j, c_{j+1}, \cdots, c_{\langle n+j-1\rangle}).$$

Without loss of generality, we suppose that $c_1 \neq 0$. From Lemma 3.1, it follows that

$$\widehat{f^{n-(l-1)}_{i,j}}(c^{n-(l-1)}) < \frac{1}{2^{l-1}}\widehat{F^n_l}(0).$$

It follows from (2.3) that $\widehat{F^n_l}(c^n)$ is the sum of $\widehat{f^{n-(l-1)}_{i,j}}(c^{n-(l-1)})$. Hence $\widehat{F^n_l}(c^n) < \widehat{F^n_l}(0)$. Namely, Theorem 1.3 is true for the case $e = 1$.

Now let $e > 1$. Let $s = \gcd(n, e)$ and $t = n/s$. Then

$$\begin{aligned} F^n_{l,e}(x^n) &= \sum_{i=1}^{n-1} x_i x_{\langle i+e\rangle} x_{\langle i+2e\rangle} \cdots x_{\langle i+(l-1)e\rangle} \\ &= \sum_{k=0}^{s-1}\sum_{j=0}^{t-1} x_{\langle k+je\rangle} x_{\langle k+je+e\rangle} x_{\langle k+je+2e\rangle} \cdots x_{\langle k+je+(l-1)e\rangle} \\ :&= \sum_{k=0}^{s-1} g^t_k(x_k, x_{\langle e+k\rangle}, ..., x_{\langle (t-1)e+k\rangle}). \end{aligned} \tag{3.2}$$

For $0 \le k \le s-1, 0 \le j \le t-1$, substituting $x_{\langle k+je\rangle}$ by $y^{(k)}_j$, one gets that

$$g^t_k(x_k, x_{\langle e+k\rangle}, ..., x_{\langle (t-1)e+k\rangle}) = \sum_{j=0}^{t-1} y^{(k)}_j y^{(k)}_{\langle j+1\rangle} y^{(k)}_{\langle j+2\rangle} \cdots y^{(k)}_{\langle j+(l-1)\rangle}.$$

Let $c^t_k = (c_k, c_{\langle e+k\rangle}, ..., c_{\langle (t-1)e+k\rangle})$ and $x^t_k = (x_k, x_{\langle e+k\rangle}, ..., x_{\langle (t-1)e+k\rangle})$. For any $c^t_k \neq 0$, we have showed that $\widehat{g^t_k}(c^t_k) < \widehat{g^t_k}(0)$. Then for all $c^n = (c_0, ..., c_{n-1}) \neq 0$, it follows from the definition of Fourier transform and (3.2) that

$$|\widehat{F^n_{l-1,e}}(c^n)| =| \sum_{i=0}^{n-1}(-1)^{x_i x_{\langle i+e\rangle} x_{\langle i+2e\rangle}\cdots x_{\langle i+(l-1)e\rangle}+c^n\cdot x^n}|$$

$$
\begin{aligned}
&=|\sum_{k=0}^{s-1}\sum_{i=0}^{t-1}(-1)^{x_{\langle k+je\rangle}x_{\langle k+je+e\rangle}\cdots x_{\langle i+je+(l-1)e\rangle}+c_k^t\cdot x_k^t}| \\
&=|\sum_{k=0}^{s-1}\widehat{g_k^t}(c_k^t)| < \sum_{k=0}^{s-1}\widehat{g_k^t}(0) = \widehat{F_{l-1,e}^n}(0).
\end{aligned}
$$

Thus Theorem 1.3 is true for the case $e > 1$.

This concludes the proof of Theorem 1.3. □

4. Final remarks

In Section 2, we present some recursive formulas for the Fourier transform of $f_{i,j}^n(x^n)$ and $F_l^n(x^n)$ for all positive integers i, j, l and n such that $l \geq 5$, $0 \leq i, j \leq l-1$ and $n \geq 2l$. So to prove the truth of Conjectures 1.1 and 1.2, it is enough to show that for any integer n such that $l \leq n \leq 2l-1$, the inequality

$$
|\widehat{f_{i,j}^n}(c^n)| < \frac{1}{2^{l-1}}\widehat{F_l^{n+l-1}}(0) \tag{4.1}
$$

is true when $c_1 = 1$. When l is an integer greater than 7 but not too large, by some direct calculations one can derive that (4.1) holds. But for the general case when $l > 7$, one meets some obstructions when one tries to prove (4.1). Hence we propose the following conjecture.

Conjecture 4.1. Let i, j, l, n be integers such that $l > 7$, $l \leq n \leq 2l-1$ and $0 \leq i, j \leq l-1$ and let $c^l = (c_0, \cdots, c_{l-1}) \in \mathbb{F}_2^l$ with $c_1 = 1$. Then

$$
|\widehat{f_{i,j}^n}(c^n)| < \frac{1}{2^{l-1}}\widehat{F_l^{n+l-1}}(0).
$$

Let $q = p^r$ with p being a prime and $r > 1$. One can form the exponential sum of a function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ as follows:

$$
S_{\mathbb{F}_q}(F) = \sum_{x\in\mathbb{F}_q^n} e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(F(x))},
$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ represents the field trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Castro, Chapman, Medina and Sepúlveda [1] showed that the sequence of $\{S_{\mathbb{F}_q}(F_l^n)\}_{n\geq l}$ satisfies the linear recurrence whose characteristic polynomial is given by

$$
X^l - q\sum_{k=0}^{l-2}(q-1)^k X^{l-2-k} = 0.
$$

On the other hand, by Lemma 2.4, we know that for any integer i and j with $0 \leq i, j \leq l-1$, the sequence $\{S_{\mathbb{F}_2}(f_{i,j}^n)\}_{n\geq l}$ satisfies the linear recurrence whose characteristic polynomial is given by

$$
X^l - 2\sum_{k=0}^{l-2} X^{l-2-k} = 0.
$$

We believe that the same holds for the general finite field. That is, we suggest the following conjecture as the conclusion of this paper.

Conjecture 4.2. Let i, j and l be integers with $l \geq 3$ and $0 \leq i, j \leq l-1$. The sequence $\{S_{\mathbb{F}_q}(f_{i,j}^n)\}_{n\geq l}$ satisfies the linear recurrence whose characteristic polynomial is given by

$$X^l - q\sum_{k=0}^{l-2}(q-1)^k X^{l-2-k} = 0.$$

Acknowledgments

The authors would like to thank the anonymous referees for careful reading of the manuscript and helpful comments and corrections that improved the presentation of this paper. Hong was supported partially by the Fundamental Research Funds for the Central Universities.

Conflict of interest

We declare that we have no conflict of interest.

References

1. F. N. Castro, R. Chapman, L. A. Medina, et al. *Recursions associated to trapezoid, symmetric and rotation symmetric functions over Galois fields*, Discrete Math. **341** (2018), 1915-1931.
2. F. N. Castro, L. A. Medina and P. Stănică, *Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent*, Appl. Algebra Eng. Comm., **29** (2018), 433–453.
3. L. C. Ciungu, *Cryptographic Boolean functions: Thus-Morse sequences, weight and nonlinearity*, Ph.D. Thesis, The State University of New York Buffalo, 2010.
4. E. Filiol and C. Fontaine, *Highly nonlinear balanced Boolean functions with a good correlation immunity*. In: International Conference on the Theory and Applications of Cryptographic Techniques, **1403** (1998), 475–488, Springer, Berlin.
5. S. Kavut, S. Maitra and M. D. Yucel, *Search for Boolean functions with excellent profiles in the rotation symmetric class,* IEEE T. Inform. Theory, **53** (2007), 1743–1751.
6. H. Kim, S. Park and S. G. Hahn, *On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2*, Discrete Appl. Math., **157** (2009), 428–432.
7. S. Mariai, T. Shimoyama and T. Kaneko, *Higher order differential attack using chosen higher order differences*, International Workshop on Selected Areas in Cryptography, **1556** (1998), 106–117, Springer-Verlag, Berlin.
8. J. Pieprzyk and C. X. Qu, *Fast hashing and rotation-symmetric functions*, J. Univers. Comput. Sci., **5** (1999), 20–31.
9. P. Stănică and S. Maitra, *Rotation symmetric Boolean functions count and cryptographic properties*, Discrete Appl. Math., **156** (2008), 1567–1580.
10. L. P. Yang, R. J. Wu and S. F. Hong, *Nonlinearity of quartic rotation symmetric Boolean functions*, Southeast Asian Bull. Math., **37** (2013), 951–961.

11. X. Zhang, H. Guo, R. Feng, et al. *Proof of a conjecture about rotation symmetric functions*, Discrete Math., **311** (2011), 1281–1289.