Proof of a conjecture about rotation symmetric functions

Xiyong Zhang\textsuperscript{a,b,*}, Hua Guo\textsuperscript{c}, Rongquan Feng\textsuperscript{d}, Yifa Li\textsuperscript{a}

\textsuperscript{a} Zhengzhou Information Science and Technology Institute, Zhengzhou, 450002, PR China
\textsuperscript{b} Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, 100191, PR China
\textsuperscript{c} School of Computer Science and Engineering, Beihang University, Beijing, 100191, PR China
\textsuperscript{d} School of Mathematical Sciences, Peking University, Beijing, 100871, PR China

A T I C L E  I N F O

Article history:
Received 29 August 2010
Received in revised form 10 March 2011
Accepted 10 March 2011
Available online 1 April 2011

Keywords:
Boolean functions
Rotation symmetric
Fourier transform
Nonlinearity

A B S T R A C T

Rotation symmetric Boolean functions have important applications in the design of cryptographic algorithms. We prove the conjecture about rotation symmetric Boolean functions (RSBFs) of degree 3 proposed in Cusick and Stănică (2002) \cite{2} and its generalization, thus the nonlinearity of such functions is determined.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

A Boolean function \( f^n(x_0, \ldots, x_{n-1}) \) on \( n \) variables is a map from \( \mathbb{F}_2^n \) to \( \mathbb{F}_2 \), where \( \mathbb{F}_2^n \) is the vector space of dimension \( n \) over the two-element field \( \mathbb{F}_2 \). Rotation symmetric Boolean functions (abbr. RSBFs) are special kinds of Boolean functions with the property that their evaluations on every cyclic inputs are the same, thus could be used as components to achieve efficient implementation in the design of a message digest algorithm in cryptography, such as MD4, MD5. These functions have attracted much attention in recent years (see \cite{3,7,6,8,4,5}). One of the main problems is to find the nonlinearity of these functions (see \cite{4,5}). It is known that a hashing algorithm employing degree-2 RSBFs as components cannot resist the linear and differential attacks \cite{6}. Hence, it is necessary to use higher-degree RSBFs with higher nonlinearity to protect the cryptography algorithm from differential attack. Cusick and Stănică \cite{2} investigated the weight of a kind of 3-degree RSBF and proposed a conjecture based on their numerical observations.

Conjecture 1.1. The nonlinearity of \( F_3^n(x_0, \ldots, x_{n-1}) = \sum_{0 \leq i \leq n-1} x_i x_{i+1(\text{mod} \ n)} x_{i+2(\text{mod} \ n)} \) is the same as its weight.

As claimed in \cite{2} if the above conjecture could be proved, then significant progress for \( k \)-degree \((k > 3)\) RSBFs might be possible. Recently, Ciungu \cite{1} proved the conjecture for the case \( 3|n \). In this paper, we factor \( F_3^n \) into four sub-functions, discover some recurrence relations, and thus prove the above conjecture. The sub-functions and related recursion formulas are different from \cite{2}. The technique used in this paper may be applied for the study of RSBFs of degree \( k > 3 \).

We define two vectors \( e_0 = (1, 0, \ldots, 0) \in \mathbb{F}_2^n \) for every \( n > 1 \), \( e_{n-1} = (0, 0, \ldots, 1) \in \mathbb{F}_2^n \), and abuse \( 0 = (0, \ldots, 0) \) to represent the zero vector in vector spaces \( \mathbb{F}_2^n \) of every dimension for simpleness. By \( x^n \) and \( c^n \) we mean the abbr. forms...
of vectors \((x_0, \ldots, x_{n-1})\) and \((c_2, \ldots, c_{n-1})\) in \(\mathbb{F}_2^n\). A linear function is of the form \(c^n \cdot x^n\), where \(\cdot\) is the vector dot product. The weight of a Boolean function \(f^n(x^n)\) is the number of solutions \(x^n \in \mathbb{F}_2^n\) such that \(f^n(x^n) = 1\), denoted by \(wt(f^n)\). The distance \(d(f^n, g^n)\) between two Boolean functions \(f^n\) and \(g^n\) is defined to be \(wt(f^n + g^n)\).

Now we list some basic definitions about Boolean functions.

**Definition 1.2.** A Boolean function \(f^n(x^n)\) is called rotation symmetric if

\[
f^n(x_0, \ldots, x_{n-1}) = f^n(x_{n-1}, x_0, x_1, \ldots, x_{n-2}) , \quad \text{for all } (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n .
\]

**Definition 1.3.** For a Boolean function \(f^n(x^n)\), the Fourier transform of \(f^n\) at \(c^n \in \mathbb{F}_2^n\) is defined as

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

By the definition of the Fourier transform, it is easy to see that

**Lemma 1.4.** For all \((c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n\),

\[
\widehat{f^n}_3(c_0, \ldots, c_{n-1}) = \widehat{f^n}_3(c_{n-1}, c_0, \ldots, c_{n-2}) .
\]

**Definition 1.5.** The nonlinearity \(N^n_f\) of a Boolean function \(f^n(x^n)\) is defined as

\[
N^n_f = \min \{ d(f^n(x^n), c^n \cdot x^n) | c^n \in \mathbb{F}_2^n \} .
\]

By **Definition 1.5**, it is not difficult to deduce that for all \(f^n(x^n)\),

\[
\widehat{f^n}(0) = 2^n - 2 \cdot wt(f^n(x^n)) .
\]

Hence we can restate the above conjecture as

\[
\widehat{f^n}_3(0) = \max \{ \|\widehat{f^n}_3(c^n)\| | c^n \in \mathbb{F}_2^n \} .
\]

**2. The proof of the conjecture**

To prove the above conjecture, we factor \(\widehat{f^n}_3\) into four sub-functions. Let

\[
t_n = \sum_{0 \leq j, k \leq n-3} x_j x_k x_{j+1} x_{k+2} \quad \text{and}
\]

\[
f^n_0(x_0, \ldots, x_{n-1}) = t_n ,
\]

\[
f^n_1(x_0, \ldots, x_{n-1}) = t_n + x_0 x_1 ,
\]

\[
f^n_2(x_0, \ldots, x_{n-1}) = t_n + x_{n-2} x_{n-1} ,
\]

\[
f^n_3(x_0, \ldots, x_{n-1}) = t_n + x_0 x_1 + x_{n-2} x_{n-1} + x_0 + x_{n-1} .
\]

Then we have

\[
\sum_{x_0, \ldots, x_{n-1}} (-1)^{f^n_3(x_0, \ldots, x_{n-1})} = \sum_{x_0, \ldots, x_{n-3}} \sum_{0 \leq j, k \leq 3} (-1)^{f^n_3(x_0, \ldots, x_{n-3})} .
\]

Next we give some recursion relations about \(\widehat{f^n_0}(c^n)\) with respect to \(n\). It should be noted that we will use these relations for \(n-2\) in this paper.

**Lemma 2.1.** For every \(c^n = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n\), if \(c_{n-1} = 0\), then

\[
\begin{align*}
\widehat{f^n_0}(c^n) &= 2 \left( \widehat{f^n_0}(c^n-2) + (-1)^{c_{n-2}} \cdot \widehat{f^n_0}(c^n-3) \right) , \\
\widehat{f^n_1}(c^n) &= 2 \left( \widehat{f^n_1}(c^n-2) + (-1)^{c_{n-2}} \cdot \widehat{f^n_1}(c^n-3) \right) , \\
\widehat{f^n_2}(c^n) &= 2 \left( \widehat{f^n_2}(c^n-2) + (-1)^{c_{n-2} + c_{n-3}} \cdot \widehat{f^n_2}(c^n-3) + c_{n-3} + e_n \right) , \\
\widehat{f^n_3}(c^n) &= 2 \left( (-1)^{c_{n-2}} \cdot \widehat{f^n_3}(c^n-3) + e_0 \right) ,
\end{align*}
\]

where \(c^n-2 \in \mathbb{F}_2^{n-2}\) and \(c^n-3 \in \mathbb{F}_2^{n-3}\) are the first \(n-2\) and \(n-3\) bits of \(c^n \in \mathbb{F}_2^n\), and \(e_0 = (1, 0, \ldots, 0)\), \(e_{n-4} = (0, \ldots, 0, 1) \in \mathbb{F}_2^{n-3}\).
Proof. We prove the first relation, since the proof of the others are similar. Because $c_{n-1} = 0$, we have

\[
\begin{align*}
\hat{f}_0^n(c^n) &= \sum_{x^n, x_{n-1} = 0} (-1)^0\binom{c^n}{x^n+c^n, x^n} + \sum_{x^n, x_{n-1} = 1} (-1)^0\binom{c^n}{x^n+c^n, x^n} \\
&= \sum_{x^n-1, x_{n-2} = 0} (-1)^0\binom{c^n-1}{x^n-1, x^n} + \sum_{x^n-1, x_{n-2} = 1} (-1)^0\binom{c^n-1}{x^n-1, x^n} \\
&= \sum_{x^n-2, x_{n-2} = 0} (-1)^0\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^0\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^0\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^0\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^0\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^0\binom{c^n-2}{x^n-2, x^n}
\end{align*}
\]

Lemma 2.2. For every $c^n = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n$, if $c_{n-1} = 1$, then for $i = 0, 2$,

\[
\begin{align*}
\hat{f}_i^n(c^n) &= \sum_{x^n, x_{n-1} = 0} (-1)^i\binom{c^n}{x^n+c^n, x^n} + \sum_{x^n, x_{n-1} = 1} (-1)^i\binom{c^n}{x^n+c^n, x^n} \\
&= \sum_{x^n-1, x_{n-2} = 0} (-1)^i\binom{c^n-1}{x^n-1, x^n} + \sum_{x^n-1, x_{n-2} = 1} (-1)^i\binom{c^n-1}{x^n-1, x^n} \\
&= \sum_{x^n-2, x_{n-2} = 0} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n}
\end{align*}
\]

and for $i = 1$,

\[
\begin{align*}
\hat{f}_i^n(c^n) &= \sum_{x^n, x_{n-1} = 0} (-1)^i\binom{c^n}{x^n+c^n, x^n} + \sum_{x^n, x_{n-1} = 1} (-1)^i\binom{c^n}{x^n+c^n, x^n} \\
&= \sum_{x^n-1, x_{n-2} = 0} (-1)^i\binom{c^n-1}{x^n-1, x^n} + \sum_{x^n-1, x_{n-2} = 1} (-1)^i\binom{c^n-1}{x^n-1, x^n} \\
&= \sum_{x^n-2, x_{n-2} = 0} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n}
\end{align*}
\]

and for $i = 3$, 

\[
\begin{align*}
\hat{f}_i^n(c^n) &= \sum_{x^n, x_{n-1} = 0} (-1)^i\binom{c^n}{x^n+c^n, x^n} + \sum_{x^n, x_{n-1} = 1} (-1)^i\binom{c^n}{x^n+c^n, x^n} \\
&= \sum_{x^n-1, x_{n-2} = 0} (-1)^i\binom{c^n-1}{x^n-1, x^n} + \sum_{x^n-1, x_{n-2} = 1} (-1)^i\binom{c^n-1}{x^n-1, x^n} \\
&= \sum_{x^n-2, x_{n-2} = 0} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n} + \sum_{x^n-2, x_{n-2} = 1} (-1)^i\binom{c^n-2}{x^n-2, x^n}
\end{align*}
\]
\[ f_0^n(\alpha^n) = \sum_{x^0, x_{n-1}=0} (-1)^{g_0^n(x^n) + \alpha^n \cdot x^n} \]

or

\[ f_0^n(\alpha^n) = \sum_{x^0, x_{n-1}=1} (-1)^{g_0^n(x^n) + \alpha^n \cdot x^n} \]

where \( g_0^n \) and \( g_0^n(x) \) are functions corresponding to \( f_0^n(\alpha^n) + \alpha^n \cdot x^n \), where \( c_{n-1} = 1, x_{n-1} = 1, j = x_{n-4} + 2x_{n-3} + 4x_{n-2} \).

We displace these functions in detail in Table 1.

By Table 1, we have

\[ \sum_{0 < j \leq 7} (-1)^{g_0^n} = \left( (-1) + (-1)^{c_{n-4} + 1} + (-1)^{c_{n-3} + 1} + (-1)^{c_{n-3} + 1} \right) f_0^n = f_0^{n-4} \]

\[ + (-1)^{c_{n-4} + 1} + (-1)^{c_{n-3} + 1} \cdot f_2^n = f_0^{n-4} + (-1)^{c_{n-4} + c_{n-3} + 1} (1 + (-1)^{c_{n-2}}) f_2^{n-4} = f_0^{n-5} + (-1)^{c_{n-4} + c_{n-3} + 1} + (-1)^{c_{n-2}} f_2^{n-5} + e_{n-5} \]

\[ = \begin{cases} 
-2(-1)^{c_{n-3}} f_0^{n-4} & \text{if } c_{n-2} = 1, \\
-2f_0^{n-4} - 4(-1)^{c_{n-4} + c_{n-5}} f_2^{n-5} & \text{if } c_{n-2} = 0, c_{n-3} = 0, \\
-2f_0^{n-4} - 4(-1)^{c_{n-4} + c_{n-5}} f_2^{n-5} + e_{n-6} & \text{if } c_{n-2} = 0, c_{n-3} = 1. 
\end{cases} \]

So we have

\[ f_0^n(\alpha^n) = \begin{cases} 
-2(-1)^{c_{n-3}} f_0^{n-4} & \text{if } c_{n-2} = 1, \\
-2f_0^{n-4} - 4(-1)^{c_{n-4} + c_{n-5}} f_2^{n-5} & \text{if } c_{n-2} = 0, c_{n-3} = 0, \\
-2f_0^{n-4} - 4(-1)^{c_{n-4} + c_{n-5}} f_2^{n-5} + e_{n-6} & \text{if } c_{n-2} = 0, c_{n-3} = 1. 
\end{cases} \]

For the proof of the relation of \( f_2^n \), we list the functions \( g_2^n \) \((0 \leq j \leq 7)\) corresponding to \( f_2^n(\alpha^n) + \alpha^n \cdot x^n \) in Table 2, where \( c_{n-1} = 1, x_{n-1} = 1, j = x_{n-4} + 2x_{n-3} + 4x_{n-2} \).

Similarly

\[ f_2^n(\alpha^n) = \sum_{x^0, x_{n-1}=0} (-1)^{f_2^n(x^n) + \alpha^n \cdot x^n} \]

or

\[ f_2^n(\alpha^n) = \sum_{x^0, x_{n-1}=1} (-1)^{f_2^n(x^n) + \alpha^n \cdot x^n} \]

and

\[ \sum_{0 < j \leq 7} (-1)^{g_2^n} = \left( (-1) + (-1)^{c_{n-2}} + (-1)^{c_{n-3} + 1} + (-1)^{c_{n-3} + c_{n-2} + 1} \right) f_0^{n-4} \]
Calculating''

\[(\text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3) = \text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 = 0\]

\[(\text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3) = \text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 = 0\]

\[(\text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3) = \text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 = 0\]

\[(\text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3) = \text{\textcolor{red}{3}}^3 - \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 + \text{\textcolor{red}{3}}^3 = 0\]

By (9) and (10), the relation for \(f_2^n\) follows.

Similarly, \(\hat{F}_1^n(c^n) = \hat{F}_1^n(c^n) + \sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n} \cdot \hat{f}_2^n(c^n) + (-1)^{\hat{s}_2^n} \cdot \hat{f}_2^n(c^n) + \hat{e}_n\), where \(\sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n}\) can be calculated as

\[
\sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n} = \begin{cases} 
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 0, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 1 \text{ and } c_{n-3} = 0, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 0 \text{ and } c_{n-3} = 1, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 1 \text{ and } c_{n-3} = 1. 
\end{cases}
\]

Similarly, \(\hat{F}_2^n(c^n) = \hat{F}_2^n(c^n) + \sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n} \cdot \hat{f}_2^n(c^n) + (-1)^{\hat{s}_2^n} \cdot \hat{f}_2^n(c^n) + \hat{e}_n\), where \(\sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n}\) can be calculated as

\[
\sum_{0 \leq j \leq 7} (-1)^{\hat{s}_2^n} = \begin{cases} 
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 0, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 1 \text{ and } c_{n-3} = 0, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 0 \text{ and } c_{n-3} = 1, \\
2(-1)^{\hat{s}_2^n} \hat{f}_1^n(c^n) + 0(-1)^{s_2^n} \hat{f}_1^n(c^n) + \hat{e}_n & \text{if } c_{n-2} = 1 \text{ and } c_{n-3} = 1. 
\end{cases}
\]

Cusick and Stănică [2] have proved that \(wt(F_0^n(x)) = 2(wt(F_3^n-2(x)) + wt(F_3^n-3(x))) + 2^n-3\), i.e., \(\hat{F}_2^n(0) = 2(\hat{F}_3^n-2(0) + \hat{F}_3^n-3(0))\) (in fact it could also be verified by Lemmas 2.1 and 2.2). The following lemma gives more relations about \(\hat{F}_2^n(0)\).

**Lemma 2.3.** \(\hat{F}_2^n(0)\) satisfies the following relationships:

\[
\hat{F}_2^n(0) = \hat{F}_2^{n-1}(0) + 2\hat{F}_3^{n-4}(0) + 4\hat{F}_3^{n-5}(0) \quad n \geq 8, \\
\hat{F}_2^{n-1}(0) \leq \hat{F}_2^n(0) \leq 2\hat{F}_3^{n-1}(0), \quad n \geq 7.
\]

**Proof.** For the first equation, by the recurrence relation \(\hat{F}_n(0) = 2(\hat{F}_n-2(0) + \hat{F}_n-3(0))\), we have for all \(n \geq 8\),

\[
\hat{F}_2^n(0) = 2(\hat{F}_2^{n-2}(0) + \hat{F}_2^{n-3}(0)), \\
\hat{F}_2^{n-1}(0) = 2(\hat{F}_3^{n-3}(0) + \hat{F}_3^{n-4}(0)), \\
2\hat{F}_3^{n-2}(0) = 4(\hat{F}_3^{n-4}(0) + \hat{F}_3^{n-5}(0)).
\]

Calculating “the first equation — the second equation + the third equation”, we obtain

\[
\hat{F}_2^n(0) = \hat{F}_2^{n-1}(0) + 2\hat{F}_3^{n-4}(0) + 4\hat{F}_3^{n-5}(0).
\]

It is obvious that \(\hat{F}_2^{n-1}(0) \leq \hat{F}_2^n(0)\) for all \(n \geq 4\). For the proof of \(\hat{F}_2^n(0) \leq 2\hat{F}_3^{n-1}(0)\), we show it by induction. From Table 3, it is true for \(n < 7\). Assume that it is true for all \(n \leq s, n, s \geq 7\), we prove it for the case \(s + 1\). Since
Lemma 2.4. Let \( c^n = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n \). If \( c_1 = 1 \), then

\[
|\hat{f}_0^n(c^n)| \leq \frac{1}{4} \cdot F_{3}^{n+2}(0). \quad (0 \leq i \leq 3, \; n \geq 9).
\]

Proof. We prove it by induction. Firstly, with the help of a computer, we verify that for all \( n \in [3, 9] \), \( c^n \neq 0 \), \( |\hat{f}_0^n(c^n)| < \frac{1}{2} \cdot F_{3}^{n+2}(0), \) \((0 \leq i \leq 3).\text{ (For example, see Table 4 for the case } n = 6. \text{ In this case } F_{3}^{n+2}(0) = F_{3}^8(0) = 96, \text{ and we see that } |\hat{f}_0^n(c^n)| < \frac{1}{2} \cdot F_{3}^8(0) = 24, \text{ (0} \leq i \leq 3).\text{ ) Assume that the claim is true for all } n < s, \text{ where } n \geq 9, s \geq 10, \text{ we now prove that it is true for } s.\)

Since \( c_1 = 1 \), we have that \( c^n, c^{n-1}, c^{n-2}, c^{n-3}, c^{n-4}, c^{n-5} \) are all not zero vectors.

If \( c_{n-1} = 0 \), then by Lemmas 2.1 and 2.3, we have

\[
|\hat{f}_0^n(c^n)| = \left|2f_{0}^{n-2}(c^{i-2}) + (-1)^{i-2}f_{0}^{n-3}(c^{i-3})\right| \\
\leq 2f_{0}^{n-2}(c^{i-2}) + 2f_{0}^{n-3}(c^{i-3}) \\
< \frac{1}{4} \cdot (2(\hat{F}_{3}^0(0) + \hat{F}_{3}^{i-2}(0))) \\
= \frac{1}{4} \cdot F_{3}^{i-2}(0).
\]

Similarly, the case for \( |\hat{f}_1^n(c^n)| < \frac{1}{2} \cdot F_{3}^{n+2}(2), \; (i = 1, 2) \) can be proven.
For the case \( i = 3 \), we have
\[
\left| \hat{f}_3^n(c^3) \right| = 2(-1)^{c_{i-2}} \cdot \hat{f}_1^{c_{i-3}}(c^{i-3} + e_0) \\
= 2 \cdot \hat{f}_1^{c_{i-3}}(c^{i-3} + e_0) \\
< \frac{1}{4} \cdot 2\hat{F}_3^{-1}(0) \\
< \frac{1}{4} \cdot (2\hat{F}_3^{-1}(0) + 2\hat{F}_3(0)) \\
= \frac{1}{4} \cdot \hat{F}_3^{i+2}(0). \tag{17}
\]

If \( c_{n-1} = 1 \), we prove the cases \( i = 0, 2 \), and leave the proof for the cases \( f_1^n, f_2^n \) to the reader since the recurrence forms are similar. By Lemma 2.2, for \( i = 0, 2 \),
\[
\hat{f}_i^n(c^n) = \hat{f}_0^{n-1}(c^{n-1}) \pm 2 \cdot \hat{f}_0^{n-4}(c^{n-4}),
\]

or
\[
\hat{f}_i^n(c^n) = \hat{f}_0^{n-1}(c^{n-1}) \pm 2 \cdot \hat{f}_0^{n-4}(c^{n-4}) \pm 4 \cdot \hat{f}_1^{n-5}(c^{n-5}), \tag{18}
\]

or
\[
\hat{f}_i^n(c^n) = \hat{f}_0^{n-1}(c^{n-1}) \pm 2 \cdot \hat{f}_0^{n-4}(c^{n-4}) \pm 4 \cdot \hat{f}_1^{n-5}(c^{n-5} + e_{n-6}).
\]

We prove the inequality for the first case and the second case, while the third case is similar. If \( \hat{f}_i^n(c^n) = \hat{f}_0^{n-1}(c^{n-1}) \pm 2 \cdot \hat{f}_0^{n-4}(c^{n-4}) \), then by Lemma 2.3 and induction,
\[
\left| \hat{f}_i^n(c^n) \right| \leq \left| \hat{f}_0^{n-1}(c^{n-1}) \right| + 2 \left| \hat{f}_0^{n-4}(c^{n-4}) \right| \\
< \frac{1}{4} \cdot (\hat{F}_3^{i+1}(0) + 2\hat{F}_3^{-2}(0)) \\
< \frac{1}{4} \cdot (2\hat{F}_3(0) + 2\hat{F}_3^{-1}(0)) \\
= \frac{1}{4} \cdot \hat{F}_3^{i+2}(0). \tag{19}
\]

When \( \hat{f}_i^n(c^n) = \hat{f}_0^{n-1}(c^{n-1}) \pm 2 \cdot \hat{f}_0^{n-4}(c^{n-4}) \pm 4 \cdot \hat{f}_1^{n-5}(c^{n-5}) \), then by Lemma 2.3 and induction again,
\[
\left| \hat{f}_i^n(c^n) \right| < \frac{1}{4} \cdot (\hat{F}_3^{i+1}(0) + 2\hat{F}_3^{-2}(0) + 4\hat{F}_3^{-3}(0)) \\
= \frac{1}{4} \cdot \hat{F}_3^{i+2}(0). \tag{20}
\]

**Theorem 2.5.** For all \( c^n = (x_0, \ldots, x_{n-1}) \neq 0 \) and all \( n \geq 3 \),
\[
\left| \hat{F}_3^n(c^n) \right| < \hat{F}_3^n(0).
\]

**Proof.** For the few cases \( n \leq 10 \), we have the correctness by the computer’s computation results. Now assume that \( n > 10 \).
Since \( c^n \neq 0 \), by Lemma 1.4, \( \hat{F}_3^n(x_0, \ldots, x_{n-1}) = \hat{F}_3^n(x_j, x_{j+1}, \ldots, x_{(n+j-1)(\text{mod} n)}) \) for all \( j \in [0, n-1] \). Thus we assume that \( c_1 = 1 \). By Lemma 2.4, we have
\[
\left| \hat{F}_3^n(c^n) \right| = \left| \hat{f}_0^{n-2}(c^{n-2}) + (-1)^{e_{n-2}} \cdot \hat{f}_2^{n-2}(c^{n-2}) + (-1)^{e_{n-1}} \cdot \hat{f}_1^{n-2}(c^{n-2}) + (-1)^{e_{n-2} + e_{n-1}} \cdot \hat{f}_3^{n-2}(c^{n-2}) \right| \\
\leq \left| \hat{f}_0^{n-2}(c^{n-2}) \right| + \left| \hat{f}_2^{n-2}(c^{n-2}) \right| + \left| \hat{f}_1^{n-2}(c^{n-2}) \right| + \left| \hat{f}_3^{n-2}(c^{n-2}) \right| \\
< \frac{1}{4} \cdot (\hat{F}_3^n(0) + \hat{F}_3^n(0) + \hat{F}_3^n(0) + \hat{F}_3^n(0)) \\
= \hat{F}_3^n(0). \tag{21}
\]

In fact, we can generalize Conjecture 1.1. For given \( 1 \leq a \leq \lfloor n/2 \rfloor - 1 \), let the permutation \( \rho \) acting on the indices’ set \( \{0, 1, \ldots, n-1\} \) be defined by
\[
\rho(i) \equiv i + a(\text{mod } n), \quad i \in \{0, 1, \ldots, n-1\}.
\]
Then the permutation $\rho$ can be decomposed as

$$
\rho = \begin{pmatrix} 0 & 1 & \cdots & n-1 \\ a & a+1 & \cdots & a-1 \\ \end{pmatrix} = \begin{pmatrix} 0 & a & \cdots & (t-1)a \\ a & 2a & \cdots & 0 \end{pmatrix} \cdots \begin{pmatrix} s-1 & s+a-1 & \cdots & s+(t-1)a+1 \\ s+a-1 & s+2a-1 & \cdots & s-1 \end{pmatrix} = \pi_0 \pi_1 \cdots \pi_{s-1}
$$

where

$$
\pi_k = \begin{pmatrix} k & a+k & \cdots & (t-1)a+k \\ a+k & 2a+k & \cdots & k \end{pmatrix}, \quad (0 \leq k \leq s-1)
$$

is a permutation cycle on \( \{k, a+k, \ldots, (t-1)a+k\} \), \( s = \gcd(n, a) \), \( t = n/s \), and

$$
k + ja = \begin{cases} k + ja & \text{if } k + ja < n, \\ k + ja \pmod{n} & \text{otherwise,} \end{cases} \quad (0 \leq k \leq s-1, \ 0 \leq j \leq t-1).
$$

(21)

By the decomposition of $\rho$, we have

$$
H_n^a(x_0, \ldots, x_{n-1}) = \sum_{0 \leq i \leq s-1} x_i X_i + a \pmod{n} X_i + 2a \pmod{n}
$$

$$
= \sum_{0 \leq k \leq s-1} \sum_{0 \leq j \leq t-1} x_{k+ja} X_{k+ja} \pmod{n} X_{k+ja+2a} \pmod{n}
$$

$$
def = \sum_{0 \leq k \leq s-1} h_k^a(x_k, x_{a+k}, \ldots, x_{(t-1)a+k}).
$$

(22)

Hence by means of the substitution of indeterminates:

$$
x_{k+ja} \rightarrow y^{(k)}_x, \quad 0 \leq k \leq s-1, \ 0 \leq j \leq t-1,
$$

we get

$$
h_k^a(x_k, x_{a+k}, \ldots, x_{(t-1)a+k}) = \sum_{0 \leq j \leq t-1} y^{(k)}_x y^{(k)}_{j+2}.
$$

Let $c_k^{(a)} = (c_k, c_{a+k}, \ldots, c_{(t-1)a+k})$, $x_k^{(a)} = (x_k, x_{a+k}, \ldots, x_{(t-1)a+k})$. For all $c_k^{(a)} \neq 0$, by Theorem 2.5 we have

$$
\left| \widehat{h}_k^a(c_k^{(a)}) \right| < \widehat{h}_k^a(0).
$$

(23)

By Definition 1.3, for all $c^{(n)} = (x_0, \ldots, x_{n-1}) \neq 0$,

$$
\left| \widehat{H}_n^a(c^{(n)}) \right| = \left| \sum_{0 \leq i \leq n-1} (-1)^{x_i x_{i+2a} + c^{(n)} x_i^2} \right|
$$

$$
= \prod_{0 \leq k \leq s-1} \sum_{0 \leq j \leq t-1} (-1)^{x_{k+ja} x_{k+j+2a} + c_k^{(a)} x_k^2}
$$

$$
= \prod_{0 \leq k \leq s-1} \widehat{h}_k^a(c_k^{(a)})
$$

$$
< \prod_{0 \leq k \leq s-1} \widehat{h}_k^a(0)
$$

$$
= \widehat{H}_n^a(0).
$$

(24)

So we have proved the result.

**Theorem 2.6.** The nonlinearity of $H_n^a(x_0, \ldots, x_{n-1}) = \sum_{0 \leq i \leq n-1} x_i X_i + a \pmod{n} X_i + 2a \pmod{n}$ is the same as its weight for all $1 \leq a \leq \lceil n/2 \rceil - 1$.

3. Conclusion

In this paper we prove the conjecture proposed in [2] that the nonlinearity of $F_n^a(x_0, \ldots, x_{n-1})$ is the same as its weight. Recently Cusick remarked that the computer’s results imply that the conjecture may be extended to RSBF with SANF $x_0 x_2 \pmod{b}$ in the case of odd $n$. However it seems difficult to prove that. It is interesting to note that it has been proved in [5] that the nonlinearity of $F_n^a(x_0, \ldots, x_{n-1}) = \sum_{0 \leq i \leq n-1} x_i X_i + s \pmod{n}$ is the same as its weight if $\frac{n}{\gcd(n,a)}$ is even.
References