The Reducibility of a Special Binary Pentanomial

Ryul Kim¹ and Yun Mi Kim²

¹ Faculty of Mathematics, Kim Il Sung University, Pyongyang, Democratic People’s Republic of Korea
² Department of Applied Mathematics, Kim Chaek University of Technology, Pyongyang, Democratic People’s Republic of Korea

Correspondence should be addressed to Ryul Kim; ryul_kim@yahoo.com

Received 30 May 2014; Accepted 20 August 2014; Published 2 September 2014

Academic Editor: Peter Fleischmann

Copyright © 2014 R. Kim and Y. M. Kim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Swan’s theorem determines the parity of the number of irreducible factors of a binary trinomial. In this work, we study the parity of the number of irreducible factors for a special binary pentanomial with even degree
\[ x^m + x^{n_1} + x^{n_2} + x^{n_3} + 1 \]
where \( 0 < n_3 < n_2 < n_1 \leq m/2 \), and exactly one of \( n_1, n_2, \) and \( n_3 \) is odd. This kind of irreducible pentanomials can be used for a fast implementation of trace and square root computations in finite fields of characteristic 2.

1. Introduction

Irreducible polynomials of low weight over a finite field are frequently used in many applications such as coding theory and cryptography due to efficient arithmetic implementation in an extension field and, thus, it is important to determine the irreducibility of such polynomials. The weight of a polynomial means the number of its nonzero coefficients.

Characterization of the parity of the number of irreducible factors of a given polynomial is of significance in this context. If a polynomial has an even number of irreducible factors, then it is reducible and, thus, the study on the parity of this number can give a necessary condition for irreducibility. Swan [1] gives the first result determining the parity of the number of irreducible factors of trinomials over \( \mathbb{F}_2 \). Vishne [2] extends Swan’s theorem to trinomials over an even-dimensional extension of \( \mathbb{F}_2 \). Many Swan-like results focus on determining the reducibility of higher weight polynomials over \( \mathbb{F}_2 \); see for example [3, 4]. Some researchers obtain the results on the reducibility of polynomials over a finite field of odd characteristic. We refer to [5, 6].

On the other hand, Ahmadi and Menezes [7] estimate the number of trace-one elements on the trinomial and pentanomial bases for a fast and low-cost implementation of trace computation. They also present a table of irreducible pentanomials whose corresponding polynomial bases have exactly one trace-one element. Each pentanomial of even degree in this table is of the form
\[ x^m + x^{n_1} + x^{n_2} + x^{n_3} + 1 \in \mathbb{F}_2[x], \]
where \( 0 < n_3 < n_2 < n_1 \leq m/2 \), and exactly one of \( n_1, n_2, \) and \( n_3 \) is odd. In this work, we characterize the parity of the number of irreducible factors of this pentanomial. We describe some preliminary results related to Swan-like results in Section 2 and determine the reducibility of the pentanomial mentioned above in Section 3.

2. Preliminaries

In this section, we recall Swan’s theorem determining the parity of the number of irreducible factors of a polynomial over \( \mathbb{F}_2 \) and some results about the discriminant and the resultant of polynomials.

Let \( \mathbb{K} \) be a field and let \( f(x) = a \prod_{i=0}^{m-1} (x - x_i) \in \mathbb{K}[x] \), where \( x_0, \ldots, x_{m-1} \) are the roots of \( f(x) \) in an extension of \( \mathbb{K} \). The discriminant of \( f(x) \) is defined by
\[ D(f) = a^{2m-2} \prod_{0 \leq i < j < m} (x_i - x_j)^2. \]

From the definition, it is clear that \( f(x) \) has a repeated root if and only if \( D(f) = 0 \). Since \( D(f) \) is a symmetric function with respect to the roots of \( f(x) \), it is an element of \( \mathbb{K} \).

The following theorem, due to Swan, relates the parity of the number of irreducible factors of a polynomial over \( \mathbb{F}_2 \) with its discriminant.
Theorem 1 (see [1, 8]). Suppose that the polynomial \( f(x) \in \mathbb{F}_2[x] \) of degree \( m \) has no repeated roots and let \( r \) be a number of irreducible factors of \( f(x) \) over \( \mathbb{F}_2 \). Let \( F(x) \in \mathbb{Z}[x] \) be any monic lift of \( f(x) \) to the integers. Then, \( D(F) \equiv 1 \) or 5 (mod 8), and \( r \equiv m \) (mod 2) if and only if \( D(F) \equiv 1 \) (mod 8).

Let \( g(x) = b\prod_{j=0}^{m-1}(x - y_j) \in \mathbb{K}[x] \), where \( y_0, \ldots, y_{m-1} \) are the roots of \( g(x) \) in an extension of \( \mathbb{K} \). The resultant of \( f(x) \) and \( g(x) \) is defined by

\[
R(f, g) = (-1)^{mn}b^m \prod_{j=0}^{m-1} f(y_j) = a^m \prod_{j=0}^{m-1} g(x_j). \tag{2}
\]

It is well known that

\[
D(f) = (-1)^{m(m-1)/2} R(f, f'), \tag{3}
\]

where \( f'(x) \) denotes the derivative of \( f(x) \) with respect to \( x \). An alternate formula for the discriminant of a monic polynomial \( f(x) \) is

\[
D(f) = (-1)^{m(m-1)/2} \prod_{i=0}^{m-1} f'(x_i), \tag{4}
\]

see [9].

Let

\[
f(x) = x^m + a_1x^{m-1} + \cdots + a_m = \prod_{i=0}^{m-1} (x - x_i) \in \mathbb{K}[x]; \tag{5}
\]

then, for all \( k, 1 \leq k < m \), the coefficients \( a_k \) of \( f(x) \)

\[
a_k = (-1)^k \sum_{0 \leq i_1 < i_2 < \cdots < i_k \leq m} x_{i_1}x_{i_2}\cdots x_{i_k} \tag{6}
\]

are the elementary symmetric polynomials of \( x_i \). Since each \( a_k \in \mathbb{K} \), it follows that \( S(x_0, \ldots, x_{m-1}) \in \mathbb{K} \) for every symmetric polynomial \( S \in \mathbb{K}[x_0, \ldots, x_{m-1}] \).

The following notation will be used throughout the paper. For all integers \( p, q \) and \( k \) (\( 0 \leq k < m \)), let

\[
S_{(k,p)} = \sum_{0 \leq i \leq m-1, i \neq p} x_i^p, \tag{7}
\]

\[
S_{(k,p)} = \sum_{0 \leq i_1 < i_2 < \cdots < i_k \leq m} x_{i_1}^p \cdots x_{i_k}^p, \tag{8}
\]

\[
S_{(p,q)} = \sum_{0 \leq i \leq m-1} x_i^p x_i^q. \tag{9}
\]

We denote \( S_{(1,p)} = S_{(1,1)} \) simply as \( S_{(p)} \) and put \( S_{(0,p)} = S_{(0,0)} = 1 \). Then, the following lemma holds.

**Lemma 2** (see [10, 11]). (1) \( S_0 = S_{(1,0)} = S_{(0,0)} = m \). (2) \( S_{p,q} = S_{(p)} S_{(q)} - S_{(p+q)} \). (3) \( S_{(p,q)} = k! \cdot S_{(p,q)} \).

The following formula, called Newton's identity, is often used for computation of the discriminant.

**Theorem 3** (see [12]). Let \( f(x), S_p, \) and \( x_0, x_1, \ldots, x_{m-1} \) be as above. Then, for every \( p \geq 1 \),

\[
S_p + S_{p-1}a_1 + S_{p-2}a_2 + \cdots + S_{p-n+1}a_{n-1} + \frac{n}{m}S_{p-n}a_n = 0, \tag{10}
\]

where \( n = \min\{p, m\} \).

The reciprocal polynomial of \( f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m \) with \( a_0 \neq 0 \) over a finite field \( \mathbb{F}_q \) is defined by

\[
f^*(x) := x^m f\left(\frac{1}{x}\right) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]. \tag{11}
\]


### 3. Main Results

In this section, we characterize the parity of the number of irreducible factors for the pentanomial

\[
f(x) = x^m + x^0 + x^{0} + x^{0} + 1 \in \mathbb{F}_2[x], \tag{12}
\]

where \( m \) is even; \( 0 < n_3 < n_2 < n_1 \leq m/2 \) and exactly one of \( n_1, n_2, \) and \( n_3 \) is odd. For our purpose, we use Swan’s theorem and Newton’s identity. In [10, 11], Newton’s identity has also been used to solve similar problems where it is enough to determine the power sums \( S_k \), with indices \( k \geq -2 \), but, for (10), one should calculate much more negative indexed power sums. We return this calculation to one of positive indexed power sums by using reciprocals.

It is clear that (10) has no repeated roots because its derivative has a unique root \( 0 \). Let \( F(x) \in \mathbb{Z}[x] \) be the monic lift of \( f(x) \) (10) to the integers and let \( x_0, \ldots, x_{m-1} \) denote the roots of \( F(x) \) in some extension of the rational numbers. The derivative of \( F(x) \) is

\[
F'(x) = mx^{m-1} + n_1x^{n_1-1} + n_2x^{n_2-1} + n_3x^{n_3-1}. \tag{13}
\]

Note that \( \prod_{i=0}^{m-1} x_i = 1 \). Our work is divided into three cases according to which one of \( n_1, n_2, \) and \( n_3 \) is odd.

**Case 1** (\( n_3 \) is odd). We can write the resultant of \( F \) and \( F' \) as

\[
R(F, F') = \prod_{i=0}^{m-1} \left(mx_i^{m-1} + n_1x_i^{n_1-1} + n_2x_i^{n_2-1} + n_3x_i^{n_3-1}\right) \tag{14}
\]

\[
\prod_{i=0}^{m-1} \left(mx_i^{m-1} + n_1x_i^{n_1-1} + n_2x_i^{n_2-1} + n_3x_i^{n_3-1}\right). \tag{15}
\]
Since \( m, n_1 \) and \( n_2 \) are even, we have
\[
R(F, F') \equiv m + mn_3 m^{-1} \sum_{i=0}^{m-1} x_i^m n_i x_{m-n_i} + n_1 n_2 m^{-2} n_3^{m-1}
\]
\[
\times \sum_{i,j} x_i^{m-n_i} x_j^{m-n_j} + n_1 n_2 m^{-1}
\]
\[
\times \sum_{i=0}^{m-1} n_i^{m-n_i} + n_1 n_2 m^{-2}
\]
\[
\times \sum_{i,j} x_i^{m-n_i} x_j^{m-n_j} + n_1 n_2 m^{-1}
\]
\[
\times \sum_{i=0}^{m-1} n_i^{m-n_i} + n_1 n_2 m^{-2}
\]
\[
\times \sum_{i,j} x_i^{m-n_i} x_j^{m-n_j} + n_1 n_2 m^{-1}
\]
\[
\times \sum_{i,j} x_i^{m-n_i} x_j^{m-n_j} \mod 16.
\] (13)

Using Lemma 2 and the fact that the square of every odd integer is congruent to 1 modulo 8, we get
\[
R(F, F') \equiv 1 + mn_3 m_{n-1} + \frac{1}{2} m^2 (S^{2}_{m-n_1} - S_{2m-2n_1})
\]
\[
+ n_1 n_3 m_{n-1} + \frac{1}{2} n_1^2 (S^{2}_{n_1-n_3} - S_{2n_1-n_2})
\]
\[
+ n_2 n_3 m_{n-1} + \frac{1}{2} n_2^2 (S^{2}_{n_2-n_3} - S_{2n_2-n_2})
\]
\[
+ mn_1 (S_{m-n_1} - S_{mn-n_1})
\]
\[
+ mn_2 (S_{m-n_2} - S_{mn-n_2})
\]
\[
+ n_1 n_2 (S_{n_1-n_2} - S_{n_1+n_2}) \mod 8.
\] (14)

Newton's identity shows that if \( 0 < k < m - n_1 \), then \( S_k = 0 \) and
\[
S_{2m-2n_1} = -(S_{m-n_1} + S_{m-n_1} + S_{mn-n_1} - S_{mn-n_1}) \mod 8.
\] (15)

Therefore,
\[
R(F, F') \equiv 1 + mn_3 m_{n-1} + \frac{1}{2} m^2 S^{2}_{m-n_1} + \frac{1}{2} m^2 S^{2}_{m-2n_1}
\]
\[
+ \frac{1}{2} m^2 S_{m-n_1} + \frac{1}{2} m^2 S_{m-n_1} - 2n_1 - 2n_2
\]
\[
+ \frac{1}{2} m^2 S_{mn-n_1} - \frac{1}{2} n_3^2 S_{2n_1-2n_2} \mod 8.
\]

Table I: The values of \( S_k \) for \( k < 2m - n_1 - n_2 \).

<table>
<thead>
<tr>
<th>( k )</th>
<th>( S_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m-n_1 )</td>
<td>( n_1 - m )</td>
</tr>
<tr>
<td>( m-n_2 )</td>
<td>( n_1 - m )</td>
</tr>
<tr>
<td>( 2m - n_1 - n_2 )</td>
<td>( m-n_1 )</td>
</tr>
<tr>
<td>( 2m - n_1 - n_2 )</td>
<td>( m-n_1 )</td>
</tr>
<tr>
<td>( 2m - n_1 - n_2 )</td>
<td>( m-n_1 )</td>
</tr>
<tr>
<td>( m )</td>
<td>( Other )</td>
</tr>
</tbody>
</table>

The indices of terms in the above equation have a relation
\[
2n_2 - 2n_1 < n_1 + n_2 - 2n_3 < 2n_1 - 2n_3 \leq m - m_3
\]
\[
< m - n_3 \leq m + n_3 < m + n_1 - 2n_3.
\] (17)

Since \( m + n_1 - 2n_3 < 2m - n_1 - n_3 \), we determine all \( S_k \) for \( k < 2m - n_1 - n_3 \) by applying Newton's identity to get Table 1.

\[
S_{2m-2n_1} = -n_1 n_2 S_{n_1+n_2} \equiv 0 \mod 8.
\] (18)

Therefore,
\[
R(F, F') \equiv 1 + m + \frac{1}{2} m^2 - \frac{1}{2} m^3 - \frac{1}{2} m^3 n_3 + \frac{1}{2} m^2 S_{m-2n_1}
\]
\[
+ \frac{1}{2} m^2 S_{mn-n_1-2n_1} + \frac{1}{2} m^2 S_{mn-n_1-2n_1}
\]
\[
- \frac{1}{2} n_3^2 S_{2n_1-2n_2} \mod 8.
\] (19)

With reference to Table 1, we can determine all unknown terms in the above equation. We consider two subcases.

**Subcase 1** \((m \) is divisible by 4). Then, we see easily that
\[
D(F) \equiv 1 + m - \frac{(-1)^{n_1/2}}{4} n_3^2 S_{2n_1-2n_2} \mod 8.
\] (20)

hence, the value of \( D(F) \) modulo 8 depends on a pair \((k_1, k_2) := (n_1 \mod 4, n_2 \mod 4)\). Let \( S := [3n_1 - 2n_2, 2n_1 + n_2 - 2n_3, n_1 - n_2 + 2n_2 - 2n_3, 3n_2 - 2n_3] \).

**Theorem 4**. Suppose that \( n_3 \) is odd and \( m \) is divisible by 4. Then, the pentanomial \( f(x) \) in (10) has an even number of irreducible factors over \( \mathbb{F}_2 \) if and only if one of the following conditions hold.
Consider

(1) $m \equiv 0 \pmod{8}$:
   
   (a) $(k_1, k_2) = (0, 0)$;
   
   (b) $(k_1, k_2) = (0, 2)$ and $m \not\equiv 3n_2 - 2n_3$;
   
   (c) $(k_1, k_2) = (2, 0)$ and $m \not\equiv 3n_1 - 2n_3$;
   
   (d) $(k_1, k_2) = (2, 2)$ and $m \not\in S$.

(2) $m \equiv 4 \pmod{8}$:

   (a) $(k_1, k_2) = (0, 2)$ and $m = 3n_2 - 2n_3$;
   
   (b) $(k_1, k_2) = (2, 0)$ and $m = 3n_1 - 2n_3$;
   
   (c) $(k_1, k_2) = (2, 2)$ and $m \in S$.

Proof. If $(k_1, k_2) = (0, 0)$, then $D(F) \equiv 1 + m = m \equiv 0 \pmod{8}$ and therefore, we have

$$ D(F) \equiv \begin{cases} 1 \pmod{8}, & m \equiv 0 \pmod{8} \\ 5 \pmod{8}, & m \equiv 4 \pmod{8}. \end{cases} \quad (21) $$

If $(k_1, k_2) = (0, 2)$, then

$$ D(F) \equiv 1 + m - \frac{1}{2} n_1^2 S_{2n_1 - 2n_3} \pmod{8} \quad (22) $$

and $2n_2 - 2n_3 \not\equiv m - n_1$. So if $2n_2 - 2n_3 = m - n_1$, that is, $m = 3n_2 - 2n_3$, then

$$ D(F) \equiv \begin{cases} 5 \pmod{8}, & m \equiv 0 \pmod{8} \\ 1 \pmod{8}, & m \equiv 4 \pmod{8}. \end{cases} \quad (23) $$

And if $m \not\equiv 3n_2 - 2n_3$, then (21) holds again. Similarly, if $(k_1, k_2) = (2, 0)$, then

$$ D(F) \equiv 1 + m - \frac{1}{2} n_1^2 S_{2n_1 - 2n_3} \pmod{8} \quad (24) $$

and $2n_1 - 2n_3 \not\equiv m - n_2$. Thus, if $2n_1 - 2n_3 = m - n_2$, that is, $m = 3n_1 - 2n_3$, then (23) holds and if $m \not\equiv 3n_2 - 2n_3$, then (21) holds. If $(k_1, k_2) = (2, 2)$, then

$$ D(F) \equiv 1 + m - \frac{1}{2} n_1^2 S_{2n_1 - 2n_3} - \frac{1}{2} n_2^2 S_{2n_2 - 2n_3} \pmod{8} \quad (25) $$

and $S_{2n_1 - 2n_3}$ or $S_{2n_2 - 2n_3}$ can be nonzero only when it is equal to either $m - n_1$ or $m - n_2$. Analyzing the possible cases shows that $m \in S$ implies (23) and $m \not\in S$ implies (21). Now, applying Swan's theorem completes the proof. \hfill \Box

Subcase 2 (m is not divisible by 4). Then, $m \equiv \pm 2 \pmod{8}$ and we can write

$$ D(F) \equiv (-1)^{m(m-1)/2} (A + B + C) \pmod{8}, \quad (26) $$

where

$$ A := 1 + m + \frac{1}{2} m^2 - \frac{1}{2} m^3 - \frac{1}{2} m^2 n_3, $$

$$ B := \frac{1}{2} m^2 (S_{m+2n_2} + S_{m+n_2} + S_{m+n_1 - 2n_3}), \quad (27) $$

$$ C := -\frac{1}{2} (n_1^2 S_{2n_1 - 2n_3} + n_2^2 S_{2n_2 - 2n_3}). $$

It is clear that if $m \equiv 2 \pmod{8}$, then

$$ A \equiv \begin{cases} 7 \pmod{8}, & n_3 \equiv 1 \pmod{4} \\ 3 \pmod{8}, & n_3 \equiv -1 \pmod{4} \end{cases} \quad (28) $$

and if $m \equiv -2 \pmod{8}$, then

$$ A \equiv \begin{cases} 3 \pmod{8}, & n_3 \equiv 1 \pmod{4} \\ 7 \pmod{8}, & n_3 \equiv -1 \pmod{4} \end{cases} \quad (29) $$

Now determine $B$ and $C$. First, assume that $m - 2n_1 = m - n_1$ that is, $n_1 = 2n_3$. Since $m + n_2 - 2n_3 < m$ and $m + n_1 - 2n_3 = m$ we have

$$ B = \frac{1}{2} m^2 (n_1 - 2m) \equiv \frac{1}{2} m^2 n_1 \equiv 4 \pmod{8}. \quad (30) $$

And then $C \equiv 0 \pmod{8}$ because $2n_2 - 2n_3 < 2n_1 - 2n_3 < m - n_1$. Next, assume that $m - 2n_1 = m - n_2$ that is, $n_2 = 2n_3$. Clearly, $S_{m+n_1-n_2} = S_n = -m$ and $m + n_1 - 2n_1 > m$. Since $m + n_1 - 2n_3 \equiv 2m - n_1 - n_2$, if $m + n_1 - 2n_3 = 2m - 2n_1$, that is, $m = 3n_1 - 2n_3$, then $S_{m+n_1-n_2} = m - n_1$ and if $m \not\equiv 3n_1 - 2n_3$, then $S_{m+n_1-n_2} = 0$. Therefore, we get

$$ B \equiv \begin{cases} 0 \pmod{8}, & m = 3n_1 - 2n_3 \\ 4 \pmod{8}, & m \not\equiv 3n_1 - 2n_3 \end{cases} \quad (31) $$

and also $C \equiv 0 \pmod{8}$ similarly. When $n_1 \not\equiv n_3$ and $n_2 \not\equiv n_3$, a similar consideration shows

$$ B \equiv \begin{cases} 4 \pmod{8}, & m \in S \\ 0 \pmod{8}, & \text{otherwise,} \end{cases} $$

$$ C \equiv \begin{cases} -\frac{1}{2} m n_1^2 \pmod{8}, & m = 2n_1 + n_2 - 2n_3 \\ 0 \pmod{8}, & \text{otherwise,} \end{cases} \quad (32) $$

Summarizing the above discussion and applying Swan's theorem, we have the following theorem.

**Theorem 5.** Suppose that $n_3$ is odd and $m \equiv \pm 2 \pmod{8}$. Then, the pentanomial $f(x)$ in (10) has an even number of irreducible factors over $\mathbb{F}_2$ if and only if one of the following conditions hold. Consider

(1) $(m \pmod{8}, n_3 \pmod{4}) = (2, -1)$ or $(-2, 1)$:

(a) $n_1 = 2n_3$;

(b) $n_2 = 2n_3$ and $m \not\equiv 3n_1 - 2n_3$;

(c) $n_1 \not\equiv 2n_3, n_2 \not\equiv 2n_3$ and either $m = 3n_1 - 2n_3$ or $m = 3n_2 - 2n_3$;

(d) $n_1 \not\equiv 2n_3, n_2 \not\equiv 2n_3$ and either $m = 2n_1 + n_2 - 2n_3, n_1 \equiv 0 \pmod{4}$ or $m = n_1 + 2n_2 - 2n_3, n_2 \equiv 0 \pmod{4}$;
(2) \((m \mod 8, n_3 \mod 4) = (2, 1)\) or \((-2, -1)\):

(a) \(n_2 = 2n_3\) and \(m = 3n_1 - 2n_2\);
(b) \(n_1 \neq 2n_3, n_2 \neq 2n_3\) and either \(m = 2n_1 + n_3 - n_2\) or \(m = n_1 + 2n_2 - n_3, n_2 \equiv 2 \mod 4\);
(c) \(n_1 \neq 2n_3, n_2 \neq 2n_3\) and \(m \not\equiv S\).

Case 2 \((n_3\) is odd\). Similarly, we have

\[ R(F, F') = \prod_{j=0}^{m-1} \left( m x_j^{m-n_2} + n_1 x_j^{n_1-n_2} + n_3 x_j^{n_3-n_2} + n_2 \right) \]

\[ = 1 + mn_2 S_{m-n_2} + \frac{1}{2} m^2 \left( S_{2m-2n_2} - S_{2m-2n_1} \right) \]

\[ + n_1 n_2 S_{n_1-n_2} + \frac{1}{2} n_2^2 \left( S_{n_1-n_2} - S_{2n_1-2n_2} \right) \]

\[ + n_3 n_2 S_{n_3-n_2} + \frac{1}{2} n_2^2 \left( S_{n_3-n_2} - S_{2n_3-2n_2} \right) \]

\[ + mn_1 \left( S_{m-n_1} - S_{n_1-n_2} - S_{m-n_2} \right) \]

\[ + mn_3 \left( S_{m-n_3} - S_{n_3-n_2} - S_{m-n_2} \right) \]

\[ + n_1 n_3 \left( S_{n_1-n_3} - S_{n_3-n_2} - S_{n_1-n_2} \right) \mod 8 \].

From Newton's identity, we see easily that \(S_{m-n_1} = n_1 - 2n_2\), \(S_{m-n_2} = n_2 - m\), \(S_{m-n_3} = n_3 - m\), and \(S_m = m\) are nonzero for \(k \equiv 0\) and \(k \equiv 1\) with \(k \leq m\) and \(m \geq 2\). To calculate \(S_k\) for negative indices, we observe

\[ F^*(x) = x^m + x^{m-n_2} + x^{m-n_3} + x^{m-n_1} + 1 \in \mathbb{Z}[x], \]

(a monic lift of the reciprocal polynomial of \(f(x)\)) to the integers. Denote the \(k\)th power sum of the roots of \(F^*(x)\) in some extension of the rational numbers by \(T_k\). Then, clearly \(S_{-k} = T_k\) for every positive integer \(k\). We can apply Newton's identity to \(T_k\) to see that \(T_k\) is equal to \(0\) for odd \(k < n_2\) and is even for even \(k < n_2\). From the above discussion, we have

\[ R(F, F') \equiv 1 + m - m^2 n_2 + \frac{1}{2} m^2 - \frac{1}{2} m^2 S_{2m-2n_2} \]

\[- \frac{1}{2} n_1^2 S_{2n_1-2n_2} - \frac{1}{2} n_2^2 T_{2n_2-2n_3} \]

\[- n_1 n_3 S_{n_1-n_3-2n_2} \mod 8 \].

First consider the case when \(n_1 + n_3 > 2n_2\).

**Theorem 6.** Suppose that \(n_2\) is odd and \(n_1 + n_3 > 2n_2\). Then, the pentanomial \(f(x)\) in (10) has an even number of irreducible factors over \(F_2\) if and only if one of the following conditions hold. Consider

(1) \(n_1 | 2n_2\):

(a) \(n_1 = 2n_2\) and \(m = 3n_1 - 2n_2\) or \(m = 2n_2 \equiv 0 \mod 8\);
(b) \(n_1 \neq 2n_2\), \(m \neq 3n_1 - 2n_2\) and either \(m \equiv 4 \mod 8\) or \(m - 2n_2 \equiv 0 \mod 8\);
(c) \(n_1 \neq 2n_2\), \(m \neq 3n_1 - 2n_2\) and either \(m \equiv 4 \mod 8\) or \(m - 2n_2 \equiv 0 \mod 8\);

(2) \(n_3 \neq 2n_2\):

(a) \(n_1 = 2n_2\), \(m = 3n_1 - 2n_2\) and \(m \equiv 4 \mod 8\);
(b) \(n_1 = 2n_2\), \(m \neq 3n_1 - 2n_2\) and \(m \equiv 0 \mod 8\) or \(m - 2n_2 \equiv 0 \mod 8\);
(c) \(n_1 \neq 2n_2\), \(m \neq 3n_1 - 2n_2\) and either \(m \equiv 4 \mod 8\) or \(m - 2n_2 \equiv 0 \mod 8\).

**Proof.** We determine the unknown terms in (35). Clearly, \(S_{n_1+n_3-2n_2} = 0\) from \(0 < n_1 + n_3 - 2n_2 < m - n_1\). Let again

\[ A := 1 + m - m^2 n_2 + \frac{1}{2} m^2, \]

\[ B := -\frac{1}{2} m^2 S_{2m-2n_2} - \frac{1}{2} n_2^2 S_{2n_2-2n_1}, \]

\[ C := -\frac{1}{2} n_2 S_{2n_2-2n_1}. \]

It is easy to see that

\[ A \equiv \begin{cases} 1 \mod 8, & m \equiv 0 \text{ or } 2 \mod 8 \\ 5 \mod 8, & m \equiv 4 \text{ or } 6 \mod 8 \end{cases} \]

We also see that \(S_{2m-2n_2} = S_{2n_2-2n_1} + (m - n_1)\) if \(n_1 = 2n_2\) and \(m \neq 3n_1 - 2n_2\) and \(m \equiv 0 \), otherwise, since \(2n_1 - 2n_2 < m - n_1\). And, by Newton's identity, we have

\[ S_{2m-2n_2} = -S_{m-n_2} - S_{n_1-n_2} - S_{n_3-n_2} - S_{m-2n_2} \]

\[ = S_{n_1-n_2} + (m + n_1 - 2n_2) a_{m-n_2-n_1} \]

\[ + (m + n_1 - 2n_2) a_{m-n_2-n_1-n_2} \]

\[ + (m - 2n_2) a_{m-2n_2} + (m - n_1). \]

With reference to the nonzero coefficients of \(F(x)\), we obtain that \(S_{2m-2n_2} = S_{2n_2-2n_1} + (m - n_1)\) if \(n_1 = 2n_2\) and \(m \neq 3n_1 - 2n_2\), thus \(S_{2m-2n_2} = n_1 - m\) and \(m \equiv 0 \mod 4\); hence \(B \equiv 0 \mod 8\). Consideration for the other cases is similar so we describe only the results: if \(n_1 = 2n_2, m \neq 3n_1 - 2n_2\), then

\[ B \equiv \begin{cases} 0 \mod 8, & m \equiv 0 \mod 4 \\ 2 \mod 8, & m \equiv 2 \mod 4, \ n_2 \equiv 1 \mod 4 \\ -2 \mod 8, & m \equiv 2 \mod 4, \ n_2 \equiv -1 \mod 4 \end{cases} \]

\[ \text{if } n_1 \neq 2n_2, m = 3n_1 - 2n_2, \text{ then} \]

\[ B \equiv \begin{cases} 4 \mod 8, & m \equiv 0 \mod 4 \\ 2 \mod 8, & m \equiv 2 \mod 4, \ n_2 \equiv 1 \mod 4 \\ -2 \mod 8, & m \equiv 2 \mod 4, \ n_2 \equiv -1 \mod 4 \end{cases} \]
and if \( n_1 \neq 2n_2, m \neq 3n_1 - 2n_2 \), then

\[
B = \begin{cases} 
0 \pmod{8}, & m \equiv 0 \pmod{4} \\
-2 \pmod{8}, & m \equiv 2 \pmod{4}, n_2 \equiv 1 \pmod{4} \\
2 \pmod{8}, & m \equiv 2 \pmod{4}, n_2 \equiv -1 \pmod{4}.
\end{cases}
\]

(41)

Next, we compute \( C \) modulo 8. If we denote the coefficient of \( x^{m-k} \) in \( F^*(x) \) by \( b_k \), then

\[
T_{2n_2-2n_3} = -T_{2n_2-3n_3} - T_{n_2-2n_3} - (2n_2 - 2n_3) b_{2n_2-2n_3}.
\]

(42)

Since \( n_2 - 2n_3 \) is odd < \( n_2 \) and \( 2n_2 - 3n_3 \) is even < \( 2n_2 \), \( T_{n_2-2n_3} = 0 \) and \( T_{2n_2-2n_3} \) is even. It follows, therefore, that \( T_{2n_2-2n_3} \equiv T_{2n_2-3n_3} + (2n_2 - 2n_3) b_{2n_2-2n_3} \pmod{4} \). Repeating this process, we get

\[
T_{2n_2-2n_3} \equiv \sum_{i=1}^{n_1} (2n_2 - i) b_{2n_2-i} \pmod{4}, \text{ where } b_{n_3} \leq 2n_2 < (l+1)n_3. \text{ Thus, we obtain}
\]

\[
C = \begin{cases} 
4 \pmod{8}, & n_3 \mid 2n_2 \\
0 \pmod{8}, & \text{otherwise.}
\end{cases}
\]

(43)

Now, Swan’s theorem is used to complete the proof.

The remaining cases when \( n_1 + n_3 = n_2 \) or \( n_1 + n_2 < n_2 \) gives the following theorems, whose proofs follow a similar way and, hence, are omitted.

**Theorem 7.** Suppose that \( n_2 \) is odd and \( n_1 + n_3 = 2n_2 \). Then, the pentanomial \( f(x) \) in (10) has an even number of irreducible factors over \( F_2 \) if and only if one of the following conditions hold.

1. \( n_3 \mid 2n_2 \), and either \( m \equiv 4 \pmod{8} \) or \( m - 2n_2 \equiv 0 \pmod{8} \);
2. \( n_3 \not\mid 2n_2 \), and either \( m \equiv 0 \pmod{8} \) or \( m - 2n_2 \equiv 4 \pmod{8} \).

**Theorem 8.** Suppose that \( n_2 \) is odd and \( n_1 + n_3 < 2n_2 \). Then, the pentanomial \( f(x) \) in (10) has an even number of irreducible factors over \( F_2 \) if and only if one of the following conditions hold. Consider

1. \( n_3 \mid 2n_2 \), \( n_3 \mid 2n_2 - n_1 \), and either \( m \equiv 0 \pmod{8} \) or \( m - 2n_2 \equiv 0 \pmod{8} \);
2. \( n_3 \not\mid 2n_2 \), \( n_3 \not\mid 2n_2 - n_1 \), and either \( m \equiv 4 \pmod{8} \) or \( m - 2n_2 \equiv 4 \pmod{8} \);
3. \( n_3 \not\mid 2n_2 \), \( n_3 \mid 2n_2 - n_1 \), \( n_3 \equiv 0 \pmod{4} \), and either \( m \equiv 0 \pmod{8} \) or \( m - 2n_2 \equiv 0 \pmod{8} \);
4. \( n_3 \not\mid 2n_2 \), \( n_3 \mid 2n_2 - n_1 \), \( n_3 \equiv 2 \pmod{4} \) and either \( m \equiv 4 \pmod{8} \) or \( m - 2n_2 \equiv 4 \pmod{8} \);
5. \( n_3 \not\mid 2n_2 \), \( n_3 \not\mid 2n_2 - n_1 \), and either \( m \equiv 0 \pmod{8} \) or \( m - 2n_2 \equiv 0 \pmod{8} \).

**Case 3 \( n_1 \) is odd.** Analogously, to Case 2, we can write the resultant of \( F(x) \) and its derivative as follows:

\[
R(F, F') = \prod_{i=0}^{m-1} \left( mx_i^{m-n_1} + n_2 x_i^{n_2-n_1} + n_3 x_i^{n_3-n_2} + n_1 \right)
\]

\[
\equiv 1 + mn_1 n_3^{m-n_1} + \frac{1}{2} m^2 \left( S_{m-n_1}^{m-n_2} - S_{2m-2n_1} \right)
\]

\[
+ n_2 n_1 T_{n_1-n_2} + \frac{1}{2} n_2^2 \left( T_{m-n_2}^{m-n_2} - T_{2m-2n_3} \right)
\]

\[
+ n_3 n_1 T_{n_1-n_2} + \frac{1}{2} n_3^2 \left( T_{m-n_2}^{m-n_2} - T_{2m-2n_3} \right)
\]

\[
+ mn_1 T_{m-n_2}^{m-n_2} - S_{m+n_2-2n_1}
\]

\[
+ mn_3 T_{m-n_2}^{m-n_2} - S_{m+n_2-2n_1}
\]

\[
+ n_2 n_3 T_{m-n_2}^{m-n_2} - T_{2m-2n_3} \pmod{8}.
\]

(44)

Straightforward calculations show that \( S_{m-n_1} = n_1 - m \) and \( S_{m+n_2-2n_1} \) and \( S_{m+n_2-2n_1} \) are even. In this case, we have also that \( T_{k} \) is equal to 0 for odd \( k < n_1 \) and is even for even \( k < 2n_1 \). It follows, therefore, that

\[
R(F, F') \equiv 1 + m - m^2 n_1 + \frac{1}{2} m^2 - \frac{1}{2} m^2 S_{2m-2n_1}
\]

\[
- \frac{1}{2} n_2^2 T_{2m-2n_1} - \frac{1}{2} n_3^2 T_{2m-2n_1} \pmod{8}.
\]

(45)

**Theorem 9.** Suppose that \( n_1 \) is odd. Then, the pentanomial \( f(x) \) in (10) has an even number of irreducible factors over \( F_2 \) if and only if one of the following conditions hold.

1. \( m = 2n_1 \) and \( E \equiv 4 \pmod{8} \);
2. \( m \not\equiv 2n_1 \), \( E \equiv 0 \pmod{8} \), and either \( m \equiv 0 \pmod{8} \) or \( m - 2n_1 \equiv 0 \pmod{8} \);
3. \( m \not\equiv 2n_1 \), \( E \equiv 4 \pmod{8} \), and either \( m \equiv 4 \pmod{8} \) or \( m - 2n_1 \equiv 4 \pmod{8} \).

**Proof.** First, we compute \( S_{2m-2n_1} \) in (45). By Newton’s identity, we get

\[
S_{2m-2n_1} = -S_{m-n_1} - S_{m-2n_1} - S_{m-2n_1} - S_{m-2n_1}
\]

\[
- S_{m-2n_1} - (2m-2n_1) a_{2m-2n_1}.
\]

(47)

Since \( m - 2n_1 < m - 2n_1 + n_3 < m - 2n_1 + n_3 < m - n_1 \), we have \( S_{m-2n_1} = S_{m-2n_1} = S_{m-2n_1} = 0 \) and \( S_{m-2n_1} = m - n_1 - (2m - 2n_1) a_{2m-2n_1} \); hence \( S_{2m-2n_1} \) is equal to \( n_1 - m \) if \( m = 2n_1 \) and equal to \( m - n_1 \) otherwise. A simple calculation shows
that if $m = 2n_1$, then $R(F, F') \equiv 3 - E \pmod{8}$. If $m \neq 2n_1$, then
\[
R(F, F') \equiv 1 + m + \frac{1}{2}m^2 - \frac{1}{2}m^2n_1 - \frac{1}{2}m^3 - E \pmod{8}
\]
and, thus, we have
\[
R(F, F') \equiv \begin{cases} 
1 - E \pmod{8}, & m \equiv 0 \pmod{8} \\
5 - E \pmod{8}, & m \equiv 4 \pmod{8} \\
7 - E \pmod{8}, & m - 2n_1 \equiv 0 \pmod{8} \\
3 - E \pmod{8}, & m - 2n_1 \equiv 4 \pmod{8} .
\end{cases}
\]
\[(48)
\]
Now applying Swan's theorem completes the proof.

4. Conclusion

We have determined the parity of the number of irreducible factors of a pentanomial (10) under the condition that $0 < n_3 < n_2 < n_1 \leq m/2$ and exactly one of $n_1, n_2, \text{and} n_3$ is odd. Our discussion is based on Swan's theorem. If $n_1$ is odd, we obtained only a result which depends on $E$ modulo 8 instead of exponents of the terms of a given pentanomial. In this case, a complete characterization of the reducibility of the given pentanomial seems to be more difficult.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors would like to thank the anonymous referees for their useful comments and suggestions.

References

Submit your manuscripts at
http://www.hindawi.com