Hindawi Publishing Corporation
Algebra
Volume 2014, Article ID 482837, 7 pages
http://dx.doi.org/10.1155/2014/482837

Research Article

The Reducibility of a Special Binary Pentanomial

Ryul Kim[1] and Yun Mi Kim[2]

[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

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

$$D(f) = a^{2m-2} \prod_{0\leq i<j<m} \left(x_i - x_j\right)^2. \tag{1}$$

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 $5 \pmod 8$, and $r \equiv m \pmod 2$ if and only if $D(F) \equiv 1 \pmod 8$.*

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

$$R(f,g) = (-1)^{mn} b^m \prod_{j=0}^{n-1} f(y_j) = a^n \prod_{i=0}^{m-1} g(x_i). \tag{2}$$

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

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m = \prod_{i=0}^{m-1}(x - x_i) \in \mathbb{K}[x]; \tag{5}$$

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

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

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 natation will be used throughout the paper. For all integers p, q and k $(0 \le k < m)$, let

$$\begin{aligned} S_{(k,p)} &= \sum_{\substack{0 \le i_1, \ldots, i_k \le m-1 \\ i_j \ne i_l}} x_{i_1}^p \cdots x_{i_k}^p, \\ S_{[k,p]} &= \sum_{0 \le i_1 < i_2 < \cdots < i_k \le m-1} x_{i_1}^p \cdots x_{i_k}^p, \\ S_{p,q} &= \sum_{\substack{0 \le i,j \le m-1 \\ i \ne j}} x_i^p x_j^q. \end{aligned} \tag{7}$$

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

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

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 $p \ge 1$,*

$$\begin{aligned} S_p + S_{p-1}a_1 + S_{p-2}a_2 + \cdots + S_{p-n+1}a_{n-1} \\ + \frac{n}{m} S_{p-n} a_n = 0, \end{aligned} \tag{8}$$

where $n = \min\{p, m\}$.

The reciprocal polynomial of $f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m$ with $a_0 \ne 0$ over a finite field $\mathbb{F}_q$ is defined by

$$\begin{aligned} f^*(x) := x^m f\left(\frac{1}{x}\right) = a_m x^m + a_{m-1} x^{m-1} \\ + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]. \end{aligned} \tag{9}$$

See Lidl and Niederreiter [12] for more details.

3. Main Results

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

$$f(x) = x^m + x^{n_1} + x^{n_2} + x^{n_3} + 1 \in \mathbb{F}_2[x], \tag{10}$$

where m is even; $0 < n_3 < n_2 < n_1 \le m/2$ 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 $k \ge -2$, 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 $f(x)$ in (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

$$F'(x) = mx^{m-1} + n_1 x^{n_1 - 1} + n_2 x^{n_2 - 1} + n_3 x^{n_3 - 1}. \tag{11}$$

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

$$\begin{aligned} R(F, F') &= \prod_{i=0}^{m-1} \left(m x_i^{m-1} + n_1 x_i^{n_1 - 1} \right. \\ &\qquad \left. + n_2 x_i^{n_2 - 1} + n_3 x_i^{n_3 - 1}\right) \\ &= \prod_{i=0}^{m-1} \left(m x_i^{m-n_3} + n_1 x_i^{n_1 - n_3} + n_2 x_i^{n_2 - n_3} + n_3\right). \end{aligned} \tag{12}$$

Since m, n_1 and n_2 are even, we have

$$\begin{aligned} R\left(F,F'\right) \equiv{}& n_3^m + mn_3^{m-1}\sum_{i=0}^{m-1} x_i^{m-n_3} + m^2 n_3^{m-2} \\ &\times \sum_{i<j} x_i^{m-n_3} x_j^{m-n_3} + n_1 n_3^{m-1} \\ &\times \sum_{i=0}^{m-1} x_i^{n_1-n_3} + n_1^2 n_3^{m-2} \\ &\times \sum_{i<j} x_i^{n_1-n_3} x_j^{n_1-n_3} + n_2 n_3^{m-1} \\ &\times \sum_{i=0}^{m-1} x_i^{n_2-n_3} + n_2^2 n_3^{m-2} \\ &\times \sum_{i<j} x_i^{n_2-n_3} x_j^{n_2-n_3} + mn_1 n_3^{m-2} \\ &\times \sum_{i\neq j} x_i^{m-n_3} x_j^{n_1-n_3} + mn_2 n_3^{m-2} \\ &\times \sum_{i\neq j} x_i^{m-n_3} x_j^{n_2-n_3} + n_1 n_2 n_3^{m-2} \\ &\times \sum_{i\neq j} x_i^{n_1-n_3} x_j^{n_2-n_3} \pmod 8 . \end{aligned} \tag{13}$$

Using Lemma 2 and the fact that the square of every odd integer is congruent to 1 modulo 8, we get

$$\begin{aligned} R\left(F,F'\right) \equiv{}& 1 + mn_3 S_{m-n_3} + \frac{1}{2}m^2\left(S_{m-n_3}^2 - S_{2m-2n_3}\right) \\ &+ n_1 n_3 S_{n_1-n_3} + \frac{1}{2}n_1^2\left(S_{n_1-n_3}^2 - S_{2n_1-2n_3}\right) \\ &+ n_2 n_3 S_{n_2-n_3} + \frac{1}{2}n_2^2\left(S_{n_2-n_3}^2 - S_{2n_2-2n_3}\right) \\ &+ mn_1\left(S_{m-n_3}\cdot S_{n_1-n_3} - S_{m+n_1-2n_3}\right) \\ &+ mn_2\left(S_{m-n_3}\cdot S_{n_2-n_3} - S_{m+n_2-2n_3}\right) \\ &+ n_1 n_2\left(S_{n_1-n_3}\cdot S_{n_2-n_3} - S_{n_1+n_2-2n_3}\right) \pmod 8 . \end{aligned} \tag{14}$$

Newton's identity shows that if $0 < k < m - n_1$, then $S_k = 0$ and

$$S_{2m-2n_3} = -\left(S_{m-2n_3} + S_{m-n_3} + S_{m+n_2-2n_3} + S_{m+n_1-2n_3}\right). \tag{15}$$

Therefore,

$$\begin{aligned} R\left(F,F'\right) \equiv{}& 1 + mn_3 S_{m-n_3} + \frac{1}{2}m^2 S_{m-n_3}^2 + \frac{1}{2}m^2 S_{m-2n_3} \\ &+ \frac{1}{2}m^2 S_{m-n_3} + \frac{1}{2}m^2 S_{m+n_2-2n_3} \\ &+ \frac{1}{2}m^2 S_{m+n_1-2n_3} - \frac{1}{2}n_1^2 S_{2n_1-2n_3} \\ &- \frac{1}{2}n_2^2 S_{2n_2-2n_3} - mn_1 S_{m+n_1-2n_3} \\ &- mn_2 S_{m+n_2-2n_3} - n_1 n_2 S_{n_1+n_2-2n_3} \pmod 8 . \end{aligned} \tag{16}$$

Table 1: The values of S_k for $k < 2m - n_1 - n_3$.

k	S_k	k	S_k
$m - n_1$	$n_1 - m$	$2m - 2n_1$	$m - n_1$
$m - n_2$	$n_2 - m$	$2m - n_1 - n_2$	$2m - n_1 - n_2$
$m - n_3$	$n_3 - m$	$2m - 2n_2$	$m - n_2$
m	$-m$	Other	0

The indices of terms in the above equation have a relation

$$\begin{aligned} 2n_2 - 2n_3 < n_1 + n_2 - 2n_3 < 2n_1 - 2n_3 \le m - 2n_3 \\ < m - n_3 < m + n_2 - 2n_3 < m + n_1 - 2n_3. \end{aligned} \tag{17}$$

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.

Note that $S_{2m-2n_2} = m - n_2$ does only cover the case of $2m - 2n_2 < 2m - n_1 - n_3$; that is, $2n_2 > n_1 + n_3$. Since $S_{m+n_1-2n_3}$, $S_{m+n_2-2n_3}$, and $S_{n_1+n_2-2n_3}$ are all even, we have

$$\begin{aligned} -mn_1 S_{m+n_1-2n_3} - mn_2 S_{m+n_2-2n_3} \\ -n_1 n_2 S_{n_1+n_2-2n_3} \equiv 0 \pmod 8 . \end{aligned} \tag{18}$$

Therefore,

$$\begin{aligned} R\left(F,F'\right) \equiv{}& 1 + m + \frac{1}{2}m^2 - \frac{1}{2}m^3 - \frac{1}{2}m^2 n_3 + \frac{1}{2}m^2 S_{m-2n_3} \\ &+ \frac{1}{2}m^2 S_{m+n_2-2n_3} + \frac{1}{2}m^2 S_{m+n_1-2n_3} \\ &- \frac{1}{2}n_1^2 S_{2n_1-2n_3} - \frac{1}{2}n_2^2 S_{2n_2-2n_3} \pmod 8 . \end{aligned} \tag{19}$$

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

$$\begin{aligned} D(F) \equiv 1 + m - \frac{1-(-1)^{n_1/2}}{4} n_1^2 S_{2n_1-2n_3} \\ - \frac{1-(-1)^{n_2/2}}{4} n_2^2 S_{2n_2-2n_3} \pmod 8 ; \end{aligned} \tag{20}$$

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

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* $m \neq 3n_2 - 2n_3$;
(c) $(k_1, k_2) = (2, 0)$ *and* $m \neq 3n_1 - 2n_3$;
(d) $(k_1, k_2) = (2, 2)$ *and* $m \notin S$.

(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 $D(F) \equiv 1 + m \pmod 8$ and, therefore, we have

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

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

$$D(F) \equiv 1 + m - \frac{1}{2} n_2^2 S_{2n_2 - 2n_3} \pmod 8 \tag{22}$$

and $2n_2 - 2n_3 \neq m - n_1$. So if $2n_2 - 2n_3 = m - n_2$, that is, $m = 3n_2 - 2n_3$, then

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

And if $m \neq 3n_2 - 2n_3$, then (21) holds again. Similarly, if $(k_1, k_2) = (2, 0)$, then

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

and $2n_1 - 2n_3 \neq m - n_2$. Thus, if $2n_1 - 2n_3 = m - n_1$, that is, $m = 3n_1 - 2n_3$, then (23) holds and if $m \neq 3n_2 - 2n_3$, then (21) holds. If $(k_1, k_2) = (2, 2)$, then

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

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 $m \notin S$ implies (21). Now, applying Swan's theorem completes the proof. □

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

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

where

$$\begin{aligned} A &:= 1 + m + \frac{1}{2} m^2 - \frac{1}{2} m^3 - \frac{1}{2} m^2 n_3, \\ B &:= \frac{1}{2} m^2 \left(S_{m - 2n_3} + S_{m + n_2 - 2n_3} + S_{m + n_1 - 2n_3} \right), \\ C &:= -\frac{1}{2} \left(n_1^2 S_{2n_1 - 2n_3} + n_2^2 S_{2n_2 - 2n_3} \right). \end{aligned} \tag{27}$$

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

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

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

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

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

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

And then $C \equiv 0 \pmod 8$ because $2n_2 - 2n_3 < 2n_1 - 2n_3 < m - n_1$. Next, assume that $m - 2n_3 = m - n_2$; that is, $n_2 = 2n_3$. Clearly, $S_{m + n_2 - 2n_3} = S_m = -m$ and $m + n_1 - 2n_3 > m$. Since $m + n_1 - 2n_3 \neq 2m - n_1 - n_2$, if $m + n_1 - 2n_3 = 2m - 2n_1$, that is, $m = 3n_1 - 2n_3$, then $S_{m + n_1 - 2n_3} = m - n_1$ and if $m \neq 3n_1 - 2n_3$, then $S_{m + n_1 - 2n_3} = 0$. Therefore, we get

$$B \equiv \begin{cases} 0 \pmod 8, & m = 3n_1 - 2n_3 \\ 4 \pmod 8, & m \neq 3n_1 - 2n_3 \end{cases} \tag{31}$$

and also $C \equiv 0 \pmod 8$, similarly. When $n_1 \neq 2n_3$ and $n_2 \neq 2n_3$, a similar consideration shows

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

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

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) $(m \bmod 8, n_3 \bmod 4) = (2, -1)$ *or* $(-2, 1)$:

(a) $n_1 = 2n_3$;
(b) $n_2 = 2n_3$ *and* $m \neq 3n_1 - 2n_3$;
(c) $n_1 \neq 2n_3, n_2 \neq 2n_3$ *and either* $m = 3n_1 - 2n_3$ *or* $m = 3n_2 - 2n_3$;
(d) $n_1 \neq 2n_3, n_2 \neq 2n_3$ *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) $(m \bmod 8, n_3 \bmod 4) = (2,1)$ *or* $(-2,-1)$:

(a) $n_2 = 2n_3$ *and* $m = 3n_1 - 2n_3$;

(b) $n_1 \neq 2n_3, n_2 \neq 2n_3$ *and either* $m = 2n_1 + n_2 - 2n_3, n_1 \equiv 2 \pmod 4$ *or* $m = n_1 + 2n_2 - 2n_3, n_2 \equiv 2 \pmod 4$;

(c) $n_1 \neq 2n_3, n_2 \neq 2n_3$ *and* $m \notin S$.

Case 2 (n_2 is odd). Similarly, we have

$$\begin{aligned} R(F,F') &= \prod_{i=0}^{m-1}\left(mx_i^{m-n_2} + n_1x_i^{n_1-n_2} + n_3x_i^{n_3-n_2} + n_2\right) \\ &\equiv 1 + mn_2S_{m-n_2} + \frac{1}{2}m^2\left(S_{m-n_2}^2 - S_{2m-2n_2}\right) \\ &\quad + n_1n_2S_{n_1-n_2} + \frac{1}{2}n_1^2\left(S_{n_1-n_2}^2 - S_{2n_1-2n_2}\right) \\ &\quad + n_3n_2S_{n_3-n_2} + \frac{1}{2}n_3^2\left(S_{n_3-n_2}^2 - S_{2n_3-2n_2}\right) \\ &\quad + mn_1\left(S_{m-n_2}\cdot S_{n_1-n_2} - S_{m+n_1-2n_2}\right) \\ &\quad + mn_3\left(S_{m-n_2}\cdot S_{n_3-n_2} - S_{m+n_3-2n_2}\right) \\ &\quad + n_1n_3\left(S_{n_1-n_2}\cdot S_{n_3-n_2} - S_{n_1+n_3-2n_2}\right) \pmod 8. \end{aligned} \tag{33}$$

From Newton's identity, we see easily that $S_{m-n_1} = n_1 - m$, $S_{m-n_2} = n_2 - m$, $S_{m-n_3} = n_3 - m$, and $S_m = -m$ are nonzero for $k \le m$ and if k is even with $k < 2m - 2n_2$, then S_k is even. To calculate S_k for negative indices, we observe

$$F^*(x) = x^m + x^{m-n_3} + x^{m-n_2} + x^{m-n_1} + 1 \in \mathbb{Z}[x], \tag{34}$$

a monic lift of the reciprocal polynomial of $f(x)$ to the integers. Denote the kth 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 $k < 2n_2$. From the above discussion, we have

$$\begin{aligned} R(F,F') &\equiv 1 + m - m^2n_2 + \frac{1}{2}m^2 - \frac{1}{2}m^2S_{2m-2n_2} \\ &\quad - \frac{1}{2}n_1^2S_{2n_1-2n_2} - \frac{1}{2}n_3^2T_{2n_2-2n_3} \\ &\quad - n_1n_3S_{n_1+n_3-2n_2} \pmod 8. \end{aligned} \tag{35}$$

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 $\mathbb{F}_2$ if and only if one of the following conditions hold.*

Consider

(1) $n_3 \mid 2n_2$:

(a) $n_1 = 2n_2, m \neq 3n_1 - 2n_2$ *and either* $m \equiv 4 \pmod 8$ *or* $m - 2n_2 \equiv 0 \pmod 8$;

(b) $n_1 \neq 2n_2, m = 3n_1 - 2n_2$ *and either* $m \equiv 0 \pmod 8$ *or* $m - 2n_2 \equiv 0 \pmod 8$;

(c) $n_1 \neq 2n_2, m \neq 3n_1 - 2n_2$ *and either* $m \equiv 4 \pmod 8$ *or* $m - 2n_2 \equiv 4 \pmod 8$;

(2) $n_3 \nmid 2n_2$:

(a) $n_1 = 2n_2, m = 3n_1 - 2n_2$, *and* $m \equiv 4 \pmod 8$;

(b) $n_1 = 2n_2, m \neq 3n_1 - 2n_2$, *and either* $m \equiv 0 \pmod 8$ *or* $m - 2n_2 \equiv 4 \pmod 8$;

(c) $n_1 \neq 2n_2, m = 3n_1 - 2n_2$, *and either* $m \equiv 4 \pmod 8$ *or* $m - 2n_2 \equiv 4 \pmod 8$;

(d) $n_1 \neq 2n_2, m \neq 3n_1 - 2n_2$, *and either* $m \equiv 0 \pmod 8$ *or* $m - 2n_2 \equiv 0 \pmod 8$.

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

$$\begin{aligned} A &:= 1 + m - m^2n_2 + \frac{1}{2}m^2, \\ B &:= -\frac{1}{2}m^2S_{2m-2n_2} - \frac{1}{2}n_1^2S_{2n_1-2n_2}, \\ C &:= -\frac{1}{2}n_3^2T_{2n_2-2n_3}. \end{aligned} \tag{36}$$

It is easy to see that

$$A \equiv \begin{cases} 1 \pmod 8, & m \equiv 0 \text{ or } 2 \pmod 8 \\ 5 \pmod 8, & m \equiv 4 \text{ or } 6 \pmod 8. \end{cases} \tag{37}$$

We also see that $S_{2n_1-2n_2}$ is equal to $n_1 - m$ if $m = 3n_1 - 2n_2$ and equal to 0, otherwise, since $2n_1 - 2n_2 < m - n_2$. And, by Newton's identity, we have

$$\begin{aligned} S_{2m-2n_2} &= -S_{m+n_1-2n_2} - S_{m-n_2} - S_{m+n_3-2n_2} - S_{m-2n_2} \\ &= S_{2n_1-2n_2} + (m + n_1 - 2n_2)\,a_{m+n_1-2n_2} \\ &\quad + (m + n_3 - 2n_2)\,a_{m+n_3-2n_2} \\ &\quad + (m - 2n_2)\,a_{m-2n_2} + (m - n_2). \end{aligned} \tag{38}$$

With reference to the nonzero coefficients of $F(x)$, we obtain that $S_{2m-2n_2} = S_{2n_1-2n_2} + 3(m - n_2)$ if $n_1 = 2n_2$ and $S_{2m-2n_2} = S_{2n_1-2n_2} + (m - n_2)$ otherwise. Now we can determine B modulo 8. If $n_1 = 2n_2$ and $m = 3n_1 - 2n_2$, then $S_{2n_1-2n_2} = n_1 - m$ and thus $S_{2m-2n_2} = 2m + n_1 - 3n_2$. Clearly $n_1 \equiv 2 \pmod 4$ and $m \equiv 0 \pmod 4$; hence $B \equiv 4 \pmod 8$. 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

$$B \equiv \begin{cases} 0 \pmod 8, & m \equiv 0 \pmod 4 \\ 2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv 1 \pmod 4 \\ -2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv -1 \pmod 4; \end{cases} \tag{39}$$

if $n_1 \neq 2n_2$, $m = 3n_1 - 2n_2$, then

$$B \equiv \begin{cases} 4 \pmod 8, & m \equiv 0 \pmod 4 \\ 2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv 1 \pmod 4 \\ -2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv -1 \pmod 4; \end{cases} \tag{40}$$

and if $n_1 \neq 2n_2, m \neq 3n_1 - 2n_2$, then

$$B \equiv \begin{cases} 0 \pmod 8, & m \equiv 0 \pmod 4 \\ -2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv 1 \pmod 4 \\ 2 \pmod 8, & m \equiv 2 \pmod 4,\ n_2 \equiv -1 \pmod 4. \end{cases} \tag{41}$$

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

$$T_{2n_2-2n_3} = -T_{2n_2-3n_3} - T_{n_2-2n_3} - (2n_2 - 2n_3)\, b_{2n_2-2n_3}. \tag{42}$$

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 $T_{2n_2-3n_3}$ 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 $T_{2n_2-2n_3} \equiv \sum_{i=2}^{l} (2n_2 - in_3) b_{2n_2-in_3} \pmod 4$, where $ln_3 \leq 2n_2 < (l+1)n_3$. Thus, we obtain

$$C \equiv \begin{cases} 4 \pmod 8, & n_3 \mid 2n_2 \\ 0 \pmod 8, & \text{otherwise.} \end{cases} \tag{43}$$

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

The remaining cases when $n_1 + n_3 = n_2$ or $n_1 + n_3 < n_2$ 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 $\mathbb{F}_2$ 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) $n_3 \nmid 2n_2$, *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 $\mathbb{F}_2$ 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) $n_3 \mid 2n_2$, $n_3 \nmid 2n_2 - n_1$, *and either* $m \equiv 4 \pmod 8$ *or* $m - 2n_2 \equiv 4 \pmod 8$;

(3) $n_3 \nmid 2n_2$, $n_3 \mid 2n_2 - n_1, n_3 \equiv 0 \pmod 4$, *and either* $m \equiv 0 \pmod 8$ *or* $m - 2n_2 \equiv 0 \pmod 8$;

(4) $n_3 \nmid 2n_2$, $n_3 \mid 2n_2 - n_1, n_3 \equiv 2 \pmod 4$ *and either* $m \equiv 4 \pmod 8$ *or* $m - 2n_2 \equiv 4 \pmod 8$;

(5) $n_3 \nmid 2n_2$, $n_3 \nmid 2n_2 - n_1$, *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:

$$\begin{aligned} R(F, F') &= \prod_{i=0}^{m-1} \left(m x_i^{m-n_1} + n_2 x_i^{n_2-n_1} + n_3 x_i^{n_3-n_2} + n_1 \right) \\ &\equiv 1 + m n_1 S_{m-n_1} + \frac{1}{2} m^2 \left(S_{m-n_1}^2 - S_{2m-2n_1} \right) \\ &\quad + n_2 n_1 T_{n_1-n_2} + \frac{1}{2} n_2^2 \left(T_{n_1-n_2}^2 - T_{2n_1-2n_2} \right) \\ &\quad + n_3 n_1 T_{n_1-n_3} + \frac{1}{2} n_3^2 \left(T_{n_1-n_3}^2 - T_{2n_1-2n_3} \right) \\ &\quad + m n_2 \left(S_{m-n_1} \cdot T_{n_1-n_2} - S_{m+n_2-2n_1} \right) \\ &\quad + m n_3 \left(S_{m-n_1} \cdot T_{n_1-n_3} - S_{m+n_3-2n_1} \right) \\ &\quad + n_2 n_3 \left(T_{n_1-n_2} \cdot T_{n_1-n_3} - T_{2n_1-n_2-n_3} \right) \pmod 8. \end{aligned} \tag{44}$$

Straightforward calculations show that $S_{m-n_1} = n_1 - m$ and $S_{m+n_2-2n_1}$ and $S_{m+n_3-2n_1}$ 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

$$\begin{aligned} R(F, F') \equiv 1 + m - m^2 n_1 + \frac{1}{2} m^2 - \frac{1}{2} m^2 S_{2m-2n_1} \\ - \frac{1}{2} n_2^2 T_{2n_1-2n_2} - \frac{1}{2} n_3^2 T_{2n_1-2n_3} \pmod 8. \end{aligned} \tag{45}$$

Now, let

$$E := \frac{1}{2} n_2^2 T_{2n_1-2n_2} + \frac{1}{2} n_3^2 T_{2n_1-2n_3}. \tag{46}$$

We present the following result for the reducibility of $f(x)$ in (10) depending on the value of E modulo 8.

Theorem 9. *Suppose that n_1 is odd. 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.*

(1) $m = 2n_1$ *and* $E \equiv 4 \pmod 8$;

(2) $m \neq 2n_1$, $E \equiv 0 \pmod 8$, *and either* $m \equiv 0 \pmod 8$ *or* $m - 2n_1 \equiv 0 \pmod 8$;

(3) $m \neq 2n_1$, $E \equiv 4 \pmod 8$, *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

$$\begin{aligned} S_{2m-2n_1} = -S_{m-n_1} - S_{m-2n_1+n_2} - S_{m-2n_1+n_3} \\ - S_{m-2n_1} - (2m - 2n_1)\, a_{2m-2n_1}. \end{aligned} \tag{47}$$

Since $m - 2n_1 < m - 2n_1 + n_3 < m - 2n_1 + n_2 < m - n_1$, we have $S_{m-2n_1+n_2} = S_{m-2n_1+n_3} = S_{m-2n_1} = 0$ and $S_{2m-2n_1} = m - n_1 - (2m - 2n_1) a_{2m-2n_1}$; 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

$$R\left(F, F'\right) \equiv 1 + m + \frac{1}{2}m^2 - \frac{1}{2}m^2 n_1 - \frac{1}{2}m^3 - E \pmod 8 \tag{48}$$

and, thus, we have

$$R\left(F, F'\right) \equiv \begin{cases} 1 - E \pmod 8, & m \equiv 0 \pmod 8 \\ 5 - E \pmod 8, & m \equiv 4 \pmod 8 \\ 7 - E \pmod 8, & m - 2n_1 \equiv 0 \pmod 8 \\ 3 - E \pmod 8, & m - 2n_1 \equiv 4 \pmod 8. \end{cases} \tag{49}$$

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, 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

[1] R. G. Swan, "Factorization of polynomials over finite fields," *Pacific Journal of Mathematics*, vol. 12, pp. 1099–1106, 1962.

[2] U. Vishne, "Factorization of trinomials over Galois fields of characteristic 2," *Finite Fields and Their Applications*, vol. 3, no. 4, pp. 370–377, 1997.

[3] R. Kim, S. Pak, and M. Sin, "Swan-like reducibility for Type I pentanomials over a binary field," *Scientific Studies and Research*, vol. 24, no. 2, pp. 249–254, 2014.

[4] Z. Zhao and X. Cao, "A note on the reducibility of binary affine polynomials," *Designs, Codes and Cryptography*, vol. 57, no. 1, pp. 83–90, 2010.

[5] R. Kim and W. Koepf, "Parity of the number of irreducible factors for composite polynomials," *Finite Fields and Their Applications*, vol. 16, no. 3, pp. 137–143, 2010.

[6] J. von zur Gathen, "Irreducible trinomials over finite fields," *Mathematics of Computation*, vol. 72, no. 244, pp. 1987–2000, 2003.

[7] O. Ahmadi and A. Menezes, "On the number of trace-one elements in polynomial bases for $\mathbb{F}_{2^n}$," *Designs, Codes and Cryptography*, vol. 37, pp. 493–507, 2005.

[8] O. Ahmadi and G. Vega, "On the parity of the number of irreducible factors of self-reciprocal polynomials over finite fields," *Finite Fields and their Applications*, vol. 14, no. 1, pp. 124–131, 2008.

[9] B. Hanson, D. Panario, and D. Thomson, "Swan-like results for binomials and trinomials over finite fields of odd characteristic," *Designs, Codes and Cryptography*, vol. 61, no. 3, pp. 273–283, 2011.

[10] O. Ahmadi and A. Menezes, "Irreducible polynomials of maximum weight," *Utilitas Mathematica*, vol. 72, pp. 111–123, 2007.

[11] W. Koepf and R. Kim, "The parity of the number of irreducible factors for some pentanomials," *Finite Fields and Their Applications*, vol. 15, no. 5, pp. 585–603, 2009.

[12] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, UK, 1st edition, 1997.