The Parity of the Number of Irreducible Factors for Some Pentanomials

Wolfram Koepf [1], Ryul Kim[2]

[1] *Department of Mathematics*
University of Kassel, Kassel, F. R. Germany
[2] *Faculty of Mathematics and Mechanics*
Kim Il Sung University, Pyongyang, D.P.R.Korea

April 25, 2008

Abstract

It is well known that Stickelberger-Swan theorem is very important for determining reducibility of polynomials over a binary field. Using this theorem it was determined the parity of the number of irreducible factors for some kinds of polynomials over a binary field, for instance, trinomials, tetranomials, self-reciprocal polynomials and so on. We discuss this problem for type II pentanomials namely $x^m + x^{n+2} + x^{n+1} + x^n + 1 \in \mathbf{F}_2[x]$. Such pentanomials can be used for efficient implementing multiplication in finite fields of characteristic two. Based on the computation of discriminant of these pentanomials with integer coefficients, it will be characterized the parity of the number of irreducible factors over $\mathbf{F}_2$ and be established the necessary conditions for the existence of this kind of irreducible pentanomials.

Keywords: Finite field, Irreducible polynomials, Type II pentanomials

1 Introduction

For purpose of efficiently implementing field arithmetic in finite field $\mathbf{F}_{2^m}$, it is desirable to take an irreducible equally spaced polynomial(ESP) of degree m over $\mathbf{F}_2$ of the form

$$x^{kd} + x^{(k-1)d} + \cdots + x^{2d} + x^d + 1$$

where $kd = m$, or an irreducible polynomial over $\mathbf{F}_2$ of degree m and low weight such as trinomial, pentanomial and so on. Unfortunately, irreducible equally spaced polynomials are very rare and an irreducible trinomial also do not always exist for a given degree m over $\mathbf{F}_2$. On the other hand, now a conjecture that there exists an irreducible pentanomial of degree m over $\mathbf{F}_2$ for each $m \geq 4$ remains open, but there exists no known value of $m \in [4, 10000]$ for which an irreducible pentanomial does not exist. In [8], type I and type II pentanomials

over $\mathbf{F}_2$ were defined as follows:

$$\text{Type I} : x^m + x^{n+1} + x^n + x + 1, \text{where } 2 \leq n \leq \lfloor m/2 \rfloor - 1$$
$$\text{Type II} : x^m + x^{n+2} + x^{n+1} + x^n + 1, \text{where } 1 \leq n \leq \lfloor m/2 \rfloor - 1$$

The authors presented the parallel multipliers for elements of $\mathbf{F}_{2^m}$ defined by these types of pentanomials. In [7], it was proposed another multiplier for elements of $\mathbf{F}_{2^m}$ defined by a type II pentanomial with better time and gate complexity compared to ones in [8]. Though type I and type II irreducible pentanomials are abundant, they do not exist for each given degree.

Stickelberger-Swan theorem is an important tool for determining reducibility of a polynomial over a finite field. Using this theorem, Swan proved in 1962 that trinomials $x^{8k}+x^m+1 \in \mathbf{F}_2[x]$ with $8k > m$ have an even number of irreducible factors and so can not be irreducible. Many researchers used this theorem for determining the parity of the number of irreducible factors of several kinds of polynomials over $\mathbf{F}_2$.[1, 3 − 5] For applying the Stickelberger-Swan theorem, it is essential to compute a discriminant of a polynomial with the integer coefficients modulo 8. In this paper we compute the discriminant of monic lift for the type II pentanomials of even degrees over $\mathbf{F}_2$ to the integers and characterize the parity of the number of irreducible factors for these pentanomials. Our main results are theorem 3-6 that show the conditions for type II pentanomials to have an even number of irreducible factors over $\mathbf{F}_2$. Using our results one can find some families of type II pentanomials that are reducible over $\mathbf{F}_2$.

2 Preliminaries

Let K be a field, and let $f(x) = a\prod_{i=0}^{m-1}(x - x_i) \in K[x]$ where $x_0, x_1, \cdots, x_{m-1}$ are the roots of $f(x)$ in a certain extension of K. Then a discriminant $D(f)$ of f is defined as follows:

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

The following theorem, called the Stickelberger-Swan theorem, is very important for determining reducibility of a polynomial over $\mathbf{F}_2$.

Theorem 1 [9] *Suppose that the polynomial $f(x) \in \mathbf{F}_2[x]$ of degree m has no repeated roots and let r be a number of irreducible factors of $f(x)$ over $\mathbf{F}_2$. Let $F(x) \in \mathbf{Z}[x]$ be any monic lift of $f(x)$ to the integers. Then $r \equiv m \pmod 2$ if and only if $D(F) \equiv 1 \pmod 8$.*

This theorem asserts that by computing the discriminant of $F(x) \in \mathbf{Z}[x]$ modulo 8, one can determine the parity of the number of irreducible factors of the polynomial $f(x)$ over $\mathbf{F}_2$. For instance, if m is even and $D(F) \equiv 1 \pmod 8$, then $f(x)$ has an even number of irreducible factors over $\mathbf{F}_2$ and therefore it is reducible over $\mathbf{F}_2$.

Now we scribe the preliminary results on the discriminant and the resultant. Let $f(x)$ be the same as above and let $g(x) = b\prod_{j=0}^{n-1}(x - y_j) \in K[x]$, where $y_0, y_1, \cdots, y_{n-1}$ are the roots of $g(x)$ in a certain extension of K. The resultant

$R(f,g)$ of $f(x)$ and $g(x)$ is

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

The resultant has the following properties.

Lemma 1 [4, 9] (1) *If* $g = fq + r, R(f,g) = R(f,r)$
(2) *If* c *is constant,* $R(f,c) = c^m = R(c,f)$
(3) $R(x,g) = g(0), R(f,-x) = f(0)$
(4) $R(f_1 f_2, g) = R(f_1,g)R(f_2,g), R(f,g_1g_2) = R(f,g_1)R(f,g_2)$

There is an important relation between the discriminant and the resultant such as

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

Now we focus to a monic polynomial

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m = \prod_{i=0}^{m-1} (x - x_i)$$

over K. It is well known that the coefficients a_k of $f(x)$ are all the elementary symmetric polynomials of x_i:

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

for $1 \le k < m$. Since each $a_k \in K$, we have that $S(x_0, x_1, \cdots, x_{m-1}) \in K$ for any symmetric polynomial $S \in K[x_0, x_1, \cdots, x_{m-1}]$. For any integers p, q and $k, 0 \le k \le m$, let

$$S_{(k,p)} = \sum_{\substack{i_1,\cdots,i_k=0 \\ i_j \ne i_l}}^{m-1} x_{i_1}^p \cdots x_{i_k}^p, S_{[k,p]} = \sum_{\substack{i_1,\cdots,i_k=0 \\ i_1 < i_2 < \cdots < i_k}}^{m-1} x_{i_1}^p \cdots x_{i_k}^p, S_{p,q} = \sum_{\substack{i,j=0 \\ i \ne j}}^{m-1} x_i^p x_j^q$$

where $i_j \ne i_l$ means that if $j \ne l$, then $i_j \ne i_l$. We denote $S_{(1,p)} = S_{[1,p]}$ simply as S_p and put $S_{(0,p)} = S_{[0,p]} = 1$. Then we have the following lemma easily.

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

Proof. It is trivial from their definition. □

Newton's formula is very useful in computing the discriminant of a polynomial.

Theorem 2 [6, *Theorem* 1.75] *Let* $f(x), S_p$ *and* $x_0, x_1, \cdots, x_{m-1}$ *be as above. Then for any* $p \ge 1$,

$$S_p + S_{p-1}a_1 + S_{p-2}a_2 + \cdots + S_{p-n+1}a_{n-1} + \frac{n}{m} S_{p-n} a_n = 0 \tag{4}$$

where $n = min(p, m)$.

3 The parity of the number of irreducible factors in case of n even

In this section we consider the parity of the number of irreducible factors of the following pentanomial

$$f(x) = x^m + x^{n+2} + x^{n+1} + x^n + 1 \in \mathbf{F}_2[x] \tag{5}$$

where both of m and n are assumed to be even and suppose that $n < m-2$. The case of n odd is more complex and it will be considered in the next section. Let $F(x) \in \mathbf{Z}[x]$ be the monic lift of $f(x)$ to the integers which has all its coefficients equal to 0 or 1. The derivative of $F(x)$ is

$$\begin{aligned} F'(x) &= mx^{m-1} + (n+2)x^{n+1} + (n+1)x^n + nx^{n-1} = \\ &= x^{n-1}\left[mx^{m-n} + (n+2)x^2 + (n+1)x + n\right] \end{aligned}$$

Let $G(x) = mx^{m-n} + (n+2)x^2 + (n+1)x + n$. Then by lemma 1 and the equation (3), we have

$$\begin{aligned} D(F) &= (-1)^{m(m-1)/2} \cdot R(F, F') = (-1)^{m(m-1)/2} \cdot R\left(F, x^{n-1}\right) \cdot R(F, G) \\ &= (-1)^{m(m-1)/2} \cdot F(0)^{n-1} \cdot R(F, G) = (-1)^{m(m-1)/2} \cdot R(F, G) \end{aligned}$$

By (2), we can write $R(F, G)$ as

$$R(F, G) = \prod_{i=0}^{m-1} (ux_i^{m-n} + vx_i^2 + wx_i + r)$$

where $u = m, v = n+2, w = n+1, r = n$ and $x_0, x_1, \cdots, x_{m-1}$ are the roots of $F(x)$. Using $\prod_{i=0}^{m-1} x_i = 1$ and the fact that u, v and r are even, we expand the above expression to get

$$\begin{aligned} R(F, G) = {} & w^m + uw^{m-1} \sum_{i=0}^{m-1} x_i^{m-n-1} + u^2 w^{m-2} \sum_{i<j} x_i^{m-n-1} x_j^{m-n-1} \\ & + vw^{m-1} \sum_{i=0}^{m-1} x_i + v^2 w^{m-2} \sum_{i<j} x_i x_j + w^{m-1} r \sum_{i=0}^{m-1} x_i^{-1} \\ & + w^{m-2} r^2 \sum_{i<j} x_i^{-1} x_j^{-1} + uvw^{m-2} \sum_{i \neq j} x_i^{m-n-1} x_j \\ & + uw^{m-2} r \sum_{i \neq j} x_i^{m-n-1} x_j^{-1} + vw^{m-2} r \sum_{i \neq j} x_i x_j^{-1} + S(x_0, x_1, \cdots x_{m-1}) \end{aligned}$$

where $S(x_0, x_1, \cdots x_{m-1})$ is an integer congruent to 0 modulo 8. Therefore

$$\begin{aligned} R(F, G) \equiv {} & w^m + uw^{m-1} S_{m-n-1} + u^2 w^{m-2} S_{[2, m-n-1]} + vw^{m-1} S_1 + \\ & + v^2 w^{m-2} S_{[2,1]} + w^{m-1} r S_{-1} + w^{m-2} r^2 S_{[2,-1]} + uvw^{m-2} S_{m-n-1,1} + \\ & + uw^{m-2} r S_{m-n-1,-1} + vw^{m-2} r S_{1,-1} \pmod 8 \end{aligned} \tag{6}$$

Divide to two cases.

Case 1. $m \leq 2n+2$ (equivalently $2(m-n-1) \leq m$)

Lemma 3 *If $m \le 2n+2$ then*

$$R(F,G) \equiv \begin{cases} -1, & m = 2n+2 \\ 1-3n-n^2, & m = n+4 \\ 1+m-m^2+\frac{1}{2}m^2(n-m), & n+4 < m < 2n+2 \end{cases} \pmod 8 \quad (7)$$

Proof. All coefficients of the polynomial $F(x)$ are 0 except $a_{m-n-2} = a_{m-n-1} = a_{m-n} = a_m = 1$ and by Newton's formula it thus satisfies $S_1 = \cdots = S_{m-n-3} = 0$. Applying Newton's formula and lemma 2 to $F(x)$ and its reciprocal $x^m F\left(x^{-1}\right)$, we can compute each term in (6) as follows.

$$S_1 = 0,\ S_{-1} = -a_{m-1} = 0,$$

$$S_2 = -(S_1 a_1 + 2a_2) = -2a_2 = \begin{cases} -2, & m-n = 4 \\ 0, & m-n > 4 \end{cases}$$

$$S_{-2} = -(S_{-1}a_{m-1} + 2a_{m-2}) = -2a_{m-2} = \begin{cases} -2, & n = 2 \\ 0, & n > 2 \end{cases}$$

$$S_{[2,1]} = \frac{1}{2}\left(S_1^2 - S_2\right) = \begin{cases} 1, & m-n = 4 \\ 0, & m-n > 4 \end{cases}$$

$$S_{[2,-1]} = \frac{1}{2}\left(S_{-1}^2 - S_{-2}\right) = \begin{cases} 1, & n = 2 \\ 0, & n > 2 \end{cases}$$

$$S_{1,-1} = S_1 \cdot S_{-1} - S_0 = -m$$

$$\begin{aligned} S_{m-n-2} &= -\left[S_{m-n-3}\cdot a_1 + \cdots + S_1 \cdot a_{m-n-3} + (m-n-2)\,a_{m-n-2}\right] \\ &= -(m-n-2) \end{aligned}$$

$$\begin{aligned} S_{m-n-1} &= -\left[S_{m-n-2}\cdot a_1 + \cdots + S_1 \cdot a_{m-n-2} + (m-n-1)\,a_{m-n-1}\right] \\ &= -(m-n-1) \end{aligned}$$

$$S_{m-n} = \begin{cases} S_4 = -(S_2 a_2 + 4a_4) = -S_2 - 4 = -2, & m-n = 4 \\ -(m-n), & m-n > 4 \end{cases}$$

$$\begin{aligned} S_{2(m-n-1)} &= -\left(S_{m-n} + S_{m-n-1} + S_{m-n-2} + 2(m-n-1)\,a_{2(m-n-1)}\right) \\ &= \begin{cases} -S_{m-n} + (m-n-1) + (m-n-2) - 2(m-n-1), & m = 2n+2 \\ -S_{m-n} + (m-n-1) + (m-n-2), & m < 2n+2 \end{cases} \\ &\equiv \begin{cases} 1 \pmod 8, & m = 6, n = 2 \\ n+1 \pmod 8, & m = 2n+2, n > 2 \\ -1 \pmod 8, & m = n+4, n > 2 \\ 3(m-n-1) \pmod 8, & n+4 < m < 2n+2 \end{cases} \end{aligned}$$

$$\begin{aligned} S_{[2,m-n-1]} &= \frac{1}{2}\left(S_{m-n-1}^2 - S_{2(m-n-1)}\right) \\ &\equiv \begin{cases} 0 \pmod 8, & m = 6, n = 2 \\ \frac{1}{2}n(n+1) \pmod 8, & m = 2n+2, n > 2 \\ 1 \pmod 8, & m = n+4, n > 2 \\ \frac{1}{2}(m-n-1)(m-n-4) \pmod 8, & n+4 < m < 2n+2 \end{cases} \end{aligned}$$

$$S_{m-n-1,1} = S_{m-n-1}\cdot S_1 - S_{m-n} = \begin{cases} 2, & m = n+4 \\ m-n, & m > n+4 \end{cases}$$

$$S_{m-n-1,-1} = S_{m-n-1}\cdot S_{-1} - S_{m-n-2} = m-n-2$$

By substitution of above values to (6) we have (7). □

Theorem 3 *If $m \leq 2n+2$, the pentanomial* (5) *has an even number of the irreducible factors over* $\mathbf{F}_2$ *if and only if one of the following conditions holds* :

(1) $m = 2n+2$

(2) $m = n+4, n \equiv 0, 2 \pmod 8$

(3) $n+4 < m < 2n+2$ *and* (*a*) $m \equiv 0 \pmod 8$, *or* (*b*) $m \equiv 2 \pmod 8, n \equiv 2, 6 \pmod 8$, *or* (*c*) $m \equiv 6 \pmod 8, n \equiv 0, 4 \pmod 8$.

Proof. The assertion of the theorem is followed by applying Theorem 1 to

$$D(F) = (-1)^{m(m-1)/2} \cdot R(F,G) \equiv$$
$$\equiv \begin{cases} 1, & m = 2n+2 \\ (-1)^{(n+4)(n+3)/2} \cdot \left(1 - 3n - n^2\right), & m = n+4 \\ (-1)^{m(m-1)/2} \cdot \left(1 + m - m^2 + \frac{1}{2}m^2 n - \frac{1}{2}m^3\right), & n+4 < m < 2n+2 \end{cases}$$
$$\pmod 8 \square$$

Corollary 1 *Let $m \leq 2n+2$ and suppose that the pentanomial* (5) *is irreducible over* $\mathbf{F}_2$.

(1) *If* $n \equiv 0 \pmod 8$, *then* $m \equiv 2, 4 \pmod 8$

(2) *If* $n \equiv 2 \pmod 8$, *then* $m \equiv 4, 6 \pmod 8$

(3) *If* $n \equiv 4 \pmod 8$, *then either* $m \equiv 2, 4 \pmod 8$ *or* $m = n+4$

(4) *If* $n \equiv 6 \pmod 8$, *then either* $m \equiv 4, 6 \pmod 8$ *or* $m = n+4$.

Case 2. $m > 2n+2$ (equivalently $2(m-n-1) > m$)

Lemma 4 *If $m > 2n+2$, then*

$$R(F,G) \equiv 1 + m - m^2 + \frac{1}{2}m^2(n-m) + \begin{cases} 4, & n = 2 \\ 0, & n > 2 \end{cases} \pmod 8 \qquad (8)$$

Proof. In this case by Newton's formula we get

$$\begin{aligned} S_{2(m-n-1)} &= -\left(S_{m-n} + S_{m-n-1} + S_{m-n-2} + S_{m-2n-2}\right) \\ &= -\left(S_{m-n} + S_{m-n-1} + S_{m-n-2}\right) \end{aligned}$$

because $S_{m-2n-2} = 0$, for $m - 2n - 2 < m - n - 2$. Since $m > 2n+2$ and n is even, $a_1 = a_2 = 0$ and therefore

$$S_1 = 0,\ S_2 = 0,\ S_{[2,1]} = \frac{1}{2}\left(S_1^2 - S_2\right) = 0,$$
$$S_{-1} = -a_{m-1} = 0,\ S_{-2} = -2a_{m-2} = \begin{cases} -2, & n = 2 \\ 0, & n > 2 \end{cases}$$
$$S_{1,-1} = -m,\ S_{[2,-1]} = \frac{1}{2}\left(S_{-1}^2 - S_{-2}\right) = \begin{cases} 1, & n = 2 \\ 0, & n > 2 \end{cases}$$
$$S_{m-n-2} = -(m-n-2),\ S_{m-n-1} = -(m-n-1),\ S_{m-n} = -(m-n)$$
$$S_{2(m-n-1)} = (m-n-2) + (m-n-1) + (m-n) = 3(m-n-1)$$
$$S_{[2,m-n-1]} = \frac{1}{2}\left(S_{m-n-1}^2 - S_{2(m-n-1)}\right) = \frac{1}{2}(m-n-1)(m-n-4)$$
$$S_{m-n-1,1} = S_{m-n-1} \cdot S_1 - S_{m-n} = m-n$$
$$S_{m-n-1,-1} = S_{m-n-1} \cdot S_{-1} - S_{m-n-2} = m-n-2.$$

From theses values we obtain

$$R(F,G) \equiv (n+1)^m - m(n+1)^{m-1}(m-n-1)$$
$$+ \frac{1}{2}m^2(n+1)^{m-2}(m-n-1)(m-n-4) + \begin{cases} (n+1)^{m-2}n^2, & n=2 \\ 0, & n>2 \end{cases}$$
$$+ m(m-n)(n+2)(n+1)^{m-2} + m(m-n-2)(n+1)^{m-2}n - m(n+2)$$
$$(n+1)^{m-2}n \equiv 1 + m - m^2 + \frac{1}{2}m^2(n-m) + \begin{cases} 4, & n=2 \\ 0, & n>2 \end{cases} \quad \square$$

Theorem 4 *If $m > 2n+2$, the pentanomial* (5) *has an even number of the irreducible factors over $\mathbf{F}_2$ if and only if one of the following conditions holds* :
(1) $n = 2, m \equiv 4, 6 \pmod 8$
(2) $n > 2$ *and* (*a*) $m \equiv 0 \pmod 8$, *or* (*b*) $m \equiv 2 \pmod 8, n \equiv 2, 6 \pmod 8$, *or* (*c*) $m \equiv 6 \pmod 8, n \equiv 0, 4 \pmod 8$.

Proof. We can obtain easily that if $n = 2$, then

$$D(F) = (-1)^{m(m-1)/2} \cdot R(F,G) \equiv$$
$$\equiv (-1)^{m(m-1)/2} \cdot \left(1 + m - m^2 + \frac{1}{2}m^2(2-m) + 4\right)$$
$$\equiv (-1)^{m(m-1)/2} \cdot \left(5 + m - \frac{1}{2}m^3\right) \pmod 8$$

and if $n > 2$, then

$$D(F) \equiv (-1)^{m(m-1)/2} \cdot \left(1 + m - m^2 + \frac{1}{2}m^2(n-m)\right) \pmod 8$$

We obtain the result by applying theorem 1 to the above congruence. $\square$

Corollary 2 *Let $m > 2n+2$ and suppose that the pentanomial* (5) *is irreducible over $\mathbf{F}_2$.*
(1) *If $n \equiv 0, 4 \pmod 8$, then $m \equiv 2, 4 \pmod 8$.*
(2) *If $n = 2$, then $m \equiv 0, 2 \pmod 8$.*
(3) *If $n \equiv 2 \pmod 8$ and $n \neq 2$,then $m \equiv 4, 6 \pmod 8$.*
(4) *If $n \equiv 6 \pmod 8$, then $m \equiv 4, 6 \pmod 8$.*

4 The parity of the number of irreducible factors in case of n odd

This section deals with the type II pentanomials

$$f(x) = x^m + x^{n+2} + x^{n+1} + x^n + 1 \in \mathbf{F}_2[x], 1 \leq n \leq \frac{m}{2} - 1 \qquad (9)$$

in the case of n odd. Let F and G be same as before. The similar consideration as previous section makes us to get

$$R(F,G) = v^m + r^m + uv^{m-1}\sum_{i=0}^{m-1} x_i^{m-n-2} + ur^{m-1}\sum_{i=0}^{m-1} x_i^{m-n}$$
$$+ v^{m-1}w\sum_{i=0}^{m-1} x_i^{-1} + wr^{m-1}\sum_{i=0}^{m-1} x_i + u^2v^{m-2}\sum_{i<j} x_i^{m-n-2}x_j^{m-n-2}$$

$$
\begin{aligned}
&+ u^2 r^{m-2} \sum_{i<j} x_i^{m-n} x_j^{m-n} + v^{m-2} w^2 \sum_{i<j} x_i^{-1} x_j^{-1} + w^2 r^{m-2} \sum_{i<j} x_i x_j \\
&+ uv^{m-2} w \sum_{i_1 \neq i_2} x_{i_1}^{m-n-2} x_{i_2}^{-1} + uwr^{m-2} \sum_{i_1 \neq i_2} x_{i_1}^{m-n} x_{i_2} \\
&+ \sum_{k=1}^{m-1} v^k r^{m-k} \sum_{j_1 < \cdots < j_k} x_{j_1}^2 \cdots x_{j_k}^2 \\
&+ \sum_{k=1}^{m-2} uv^k r^{m-k-1} \sum_{\substack{i \neq j_1, \cdots, j_k \\ j_1 < \cdots < j_k}} x_i^{m-n} x_{j_1}^2 \cdots x_{j_k}^2 \\
&+ \sum_{k=1}^{m-3} u^2 v^k r^{m-k-2} \sum_{\substack{i_1 < i_2, j_1 < \cdots < j_k \\ i_1, i_2 \neq j_1, \cdots, j_k}} x_{i_1}^{m-n} x_{i_2}^{m-n} x_{j_1}^2 \cdots x_{j_k}^2 \\
&+ \sum_{k=1}^{m-2} v^k w r^{m-k-1} \sum_{\substack{i \neq j_1, \cdots, j_k \\ j_1 < \cdots < j_k}} x_i x_{j_1}^2 \cdots x_{j_k}^2 \\
&+ \sum_{k=1}^{m-3} v^k w^2 r^{m-k-2} \sum_{\substack{i_1 < i_2, j_1 < \cdots < j_k \\ i_1, i_2 \neq j_1, \cdots, j_k}} x_{i_1} x_{i_2} x_{j_1}^2 \cdots x_{j_k}^2 \\
&+ \sum_{k=1}^{m-3} uv^k w r^{m-k-2} \sum_{\substack{i_1 \neq i_2, j_1 < \cdots < j_k \\ i_1, i_2 \neq j_1, \cdots, j_k}} x_{i_1}^{m-n} x_{i_2} x_{j_1}^2 \cdots x_{j_k}^2 + S\left(x_0, x_1, \cdots, x_{m-1}\right)
\end{aligned}
$$

where $S\left(x_0, x_1, \cdots x_{m-1}\right)$ is an integer congruent to 0 modulo 8. Now denote respectively S, V, W, X, Y, Z the last 6 sums of above equation, and we rewrite it as

$$
\begin{aligned}
R(F,G) = {} & v^m + r^m + uv^{m-1} \sum_{i=0}^{m-1} x_i^{m-n-2} + ur^{m-1} \sum_{i=0}^{m-1} x_i^{m-n} \\
& + v^{m-1} w \sum_{i=0}^{m-1} x_i^{-1} + wr^{m-1} \sum_{i=0}^{m-1} x_i + u^2 v^{m-2} \sum_{i<j} x_i^{m-n-2} x_j^{m-n-2} \\
& + u^2 r^{m-2} \sum_{i<j} x_i^{m-n} x_j^{m-n} + v^{m-2} w^2 \sum_{i<j} x_i^{-1} x_j^{-1} + w^2 r^{m-2} \sum_{i<j} x_i x_j \\
& + uv^{m-2} w \sum_{i_1 \neq i_2} x_{i_1}^{m-n-2} x_{i_2}^{-1} + uwr^{m-2} \sum_{i_1 \neq i_2} x_{i_1}^{m-n} x_{i_2} \\
& + S + V + W + X + Y + Z.
\end{aligned}
$$

And we use the notations in section 2 to get

$$
\begin{aligned}
R(F,G) \equiv {} & v^m + r^m + uv^{m-1} \cdot S_{m-n-2} + ur^{m-1} \cdot S_{m-n} + v^{m-1} w \cdot S_{-1} \\
& + wr^{m-1} \cdot S_1 + u^2 v^{m-2} \cdot S_{[2,m-n-2]} + u^2 r^{m-2} \cdot S_{[2,m-n]} + v^{m-2} w^2 \\
& \cdot S_{[2,-1]} + w^2 r^{m-2} \cdot S_{[2,1]} + uv^{m-2} w \cdot S_{m-n-2,-1} + uwr^{m-2} \cdot S_{m-n,1} \\
& + S + V + W + X + Y + Z \pmod 8
\end{aligned}
$$

It is necessary to compute the values of S, V, W, X, Y and Z modulo 8 to characterize $R(F,G)$.

Let

$$V_k = \sum_{\substack{i\neq j_1,\cdots,j_k \\ j_1<\cdots<j_k}} x_i^{m-n}x_{j_1}^2\cdots x_{j_k}^2,\ 1\le k\le m-2$$

$$W_k = \sum_{\substack{i_1<i_2,j_1<\cdots<j_k \\ i_1,i_2\neq j_1,\cdots,j_k}} x_{i_1}^{m-n}x_{i_2}^{m-n}x_{j_1}^2\cdots x_{j_k}^2,\ 1\le k\le m-3$$

$$X_k = \sum_{\substack{i\neq j_1,\cdots,j_k \\ j_1<\cdots<j_k}} x_i x_{j_1}^2\cdots x_{j_k}^2,\ 1\le k\le m-2$$

$$Y_k = \sum_{\substack{i_1<i_2,j_1<\cdots<j_k \\ i_1,i_2\neq j_1,\cdots,j_k}} x_{i_1}x_{i_2}x_{j_1}^2\cdots x_{j_k}^2,\ 1\le k\le m-3$$

$$Z_k = \sum_{\substack{i_1\neq i_2,j_1<\cdots<j_k \\ i_1,i_2\neq j_1,\cdots,j_k}} x_{i_1}^{m-n}x_{i_2}x_{j_1}^2\cdots x_{j_k}^2,\ 1\le k\le m-3$$

For a fixed integer $i, 1\le i<m$, and for each positive integer p, let

$$U_{k,p} = U_{k,p}^i = \sum_{\substack{i\neq j_1,\cdots,j_k \\ j_l\neq j_t}} x_{j_1}^p\cdots x_{j_k}^p$$

and put $U_{0,p}=1$ for any p. Then we obtain the following lemmas.

Lemma 5

$$U_{k,p} = \sum_{j=0}^{k}(-1)^j\frac{k!}{(k-j)!}\cdot x_i^{jp}\cdot S_{(k-j,p)}$$

Proof. From definition of $U_{k,p}$, we have

$$\begin{aligned}
U_{k,p} &= \sum_{j_l\neq j_t} x_{j_1}^p\cdots x_{j_k}^p - kx_i^p\sum_{\substack{i\neq j_1,\cdots,j_{k-1} \\ j_l\neq j_t}} x_{j_1}^p\cdots x_{j_{k-1}}^p \\
&= S_{(k,p)} - kx_i^p\cdot U_{k-1,p} = S_{(k,p)} - kx_i^p\left(S_{(k-1,p)} - (k-1)x_i^pU_{k-2,p}\right) \\
&= S_{(k,p)} - kx_i^p\cdot S_{(k-1,p)} + k(k-1)x_i^{2p}\cdot U_{k-2,p} = \cdots = \\
&= S_{(k,p)} - kx_i^p\cdot S_{(k-1,p)} + k(k-1)x_i^{2p}\cdot S_{(k-2,p)} + \cdots + \\
&+ (-1)^{k-1}\cdot k(k-1)\cdots 2\cdot x_i^{(k-1)p}\left(S_{(1,p)} - 1\cdot x_i^p\right) \\
&= \sum_{j=0}^{k}(-1)^j\frac{k!}{(k-j)!}\cdot x_i^{jp}\cdot S_{(k-j,p)}\square
\end{aligned}$$

Lemma 6

$$S_{(k,p)}\cdot S_p = S_{(k+1,p)} + \sum_{j=1}^{k}(-1)^{j+1}\frac{k!}{(k-j)!}\cdot S_{(j+1)p}\cdot S_{(k-j,p)}$$

Proof.

$$S_{(k,p)} \cdot S_p = \left(\sum_{j_l \neq j_t} x_{j_1}^p \cdots x_{j_k}^p \right) \left(\sum_{i=0}^{m-1} x_i^p \right) = \sum_{i=0}^{m-1} k x_i^{2p} \cdot U_{k-1,p} + S_{(k+1,p)}$$

$$= S_{(k+1,p)} + \sum_{i=0}^{m-1} k x_i^{2p} \cdot \left(\sum_{j=0}^{k-1} (-1)^j \frac{(k-1)!}{(k-j-1)!} \cdot x_i^{jp} \cdot S_{(k-j-1,p)} \right)$$

$$= S_{(k+1,p)} + \sum_{j=1}^{k} \sum_{i=0}^{m-1} (-1)^{j-1} \frac{k!}{(k-j)!} \cdot x_i^{(j+1)p} \cdot S_{(k-j,p)}$$

$$= S_{(k+1,p)} + \sum_{j=1}^{k} (-1)^{j+1} \frac{k!}{(k-j)!} \cdot S_{(j+1)p} \cdot S_{(k-j,p)} \square$$

By applying Newton's formula and these lemmas we compute S, V, W, X, Y, and Z modulo 8. For simplicity we assume in this section that m and n are large, for example, $n > 4$ and $m > 4(n-2)$. Suppose that m is not dividable by 4. If m is multiple of 4, then it is similar and simpler.

4.1 Computation of S

First we compute the non-zero values of S_p by Newton's formula similarly as previous section. The following table shows the non-zero values of S_p for $p \in [1, 4m-3n]$. These are needed for below computation.

p	S_p	p	S_p
$m-n-2$	$-(m-n-2)$	$3m-2n-1$	$-2(3m-2n-1)$
$m-n-1$	$-(m-n-1)$	$3m-2n$	$-(3m-2n)$
$m-n$	$-(m-n)$	$3m-n-2$	$-(3m-n-2)$
m	$-m$	$3m-n-1$	$-(3m-n-1)$
$2(m-n-2)$	$m-n-2$	$3m-n$	$-(3m-n)$
$2m-2n-3$	$2m-2n-3$	$3m$	$-m$
$2m-2n-2$	$3(m-n-1)$	$4(m-n-2)$	$m-n-2$
$2m-2n-1$	$2m-2n-1$	$4m-4n-7$	$4m-4n-7$
$2m-2n$	$m-n$	$4m-4n-6$	$5(2m-2n-3)$
$2m-n-2$	$2m-n-2$	$4m-4n-5$	$4(4m-4n-5)$
$2m-n-1$	$2m-n-1$	$4m-4n-4$	$19(m-n-1)$
$2m-n$	$2m-n$	$4m-4n-3$	$4(4m-4n-3)$
$2m$	m	$4m-4n-2$	$5(2m-2n-1)$
$3(m-n-2)$	$-(m-n-2)$	$4m-4n-1$	$4m-4n-1$
$3m-3n-5$	$-(3m-3n-5)$	$4m-4n$	$m-n$
$3m-3n-4$	$-2(3m-3n-4)$	$4m-3n-6$	$4m-3n-6$
$3m-3n-3$	$-7(m-n-1)$	$4m-3n-5$	$3(4m-3n-5)$
$3m-3n-2$	$-2(3m-3n-2)$	$4m-3n-4$	$6(4m-3n-4)$
$3m-3n-1$	$-(3m-3n-1)$	$4m-3n-3$	$7(4m-3n-3)$
$3m-3n$	$-(m-n)$	$4m-3n-2$	$6(4m-3n-2)$
$3m-2n-4$	$-(3m-2n-4)$	$4m-3n-1$	$3(4m-3n-1)$
$3m-2n-3$	$-2(3m-2n-3)$	$4m-3n$	$4m-3n$
$3m-2n-2$	$-3(3m-2n-2)$		

From these values we compute $S_{(k,2)}$ for $1 \le k \le m$ by applying lemma 6. If $1 \le k < \frac{m-n-1}{2}$, we see that $S_{(k,2)} = 0$.

$$\begin{aligned}
S_{(\frac{m-n-1}{2},2)} &= (-1)^{\frac{m-n-1}{2}-1} \cdot \left(\frac{m-n-3}{2}\right)! \cdot S_{m-n-1} \\
&= (-1)^{\frac{m-n-1}{2}} \cdot 2\left(\frac{m-n-1}{2}\right)! \\
S_{(\frac{m}{2},2)} &= (-1)^{\frac{m-n-3}{2}} \cdot \frac{\left(\frac{m}{2}-1\right)!}{\left(\frac{m}{2}-\frac{m-n-1}{2}\right)!} \cdot S_{\left(\frac{m}{2}-\frac{m-n-1}{2},2\right)} \cdot S_{m-n-1} \\
&= (-1)^{\frac{m}{2}} \cdot 2\left(\frac{m}{2}\right)! \\
S_{(m-n-2,2)} &= (-1)^{m-n-3} \cdot (m-n-3)! \cdot S_{2(m-n-2)} \\
&= (-1)^{m-n-3} \cdot (m-n-2)! \\
S_{(m-n-1,2)} &= (-1)^{\frac{m-n-3}{2}} \cdot \frac{(m-n-2)!}{\left(\frac{m-n-1}{2}\right)!} \cdot S_{\left(\frac{m-n-1}{2},2\right)} \cdot S_{m-n-1} \\
&\quad + (-1)^{m-n-2} \cdot (m-n-2)! \cdot S_{2(m-n-1)} = (-1)^{m-n-2} \cdot (m-n-1)! \\
S_{(m-n,2)} &= (-1)^{\frac{m-n-3}{2}} \cdot \frac{(m-n-1)!}{\left(\frac{m-n+1}{2}\right)!} \cdot S_{\left(\frac{m-n+1}{2},2\right)} \cdot S_{m-n-1} \\
&\quad + (-1)^{m-n-1} \cdot (m-n-1)! \cdot S_{2(m-n)} = (-1)^{m-n-1} \cdot (m-n)! \\
S_{(\frac{2m-n-1}{2},2)} &= (-1)^{\frac{m-n-3}{2}} \cdot \frac{\left(\frac{2m-n-3}{2}\right)!}{\left(\frac{m}{2}\right)!} \cdot S_{\left(\frac{m}{2},2\right)} \cdot S_{m-n-1} \\
&\quad + (-1)^{\frac{m}{2}-1} \cdot \frac{\left(\frac{2m-n-3}{2}\right)!}{\left(\frac{m-n-1}{2}\right)!} \cdot S_{\left(\frac{m-n-1}{2},2\right)} \cdot S_m + (-1)^{\frac{2m-n-3}{2}} \cdot \left(\frac{2m-n-3}{2}\right)! \\
&\quad \cdot S_{2m-n-1} = (-1)^{\frac{2m-n-1}{2}} \cdot 2 \cdot \left(\frac{2m-n-1}{2}\right)! \\
S_{(m,2)} &= (-1)^{\frac{m}{2}-1} \cdot \frac{(m-1)!}{\left(\frac{m}{2}\right)!} \cdot S_{\left(\frac{m}{2},2\right)} \cdot S_m + (-1)^{m-1} \cdot (m-1)! \cdot S_{2m} \\
&= (-1)^m \cdot m! = m!
\end{aligned}$$

Now we are ready to compute S modulo 8. Throughout this section we often use the fact that the quadrate of each odd integer is congruent to 1 modulo 8.

Lemma 7 $S \equiv (-1)^{\frac{n+1}{2}} \cdot 4 \cdot (n+2)^{\frac{n-1}{2}} \cdot n^{\frac{n+1}{2}} - 1 \pmod 8$

Proof.

$$\begin{aligned}
S = \sum_{k=1}^{m-1} v^k \cdot r^{m-k} \cdot S_{[k,2]} &\equiv v^{\frac{m-n-1}{2}} \cdot r^{\frac{m+n+1}{2}} \cdot S_{\left[\frac{m-n-1}{2},2\right]} + v^{\frac{m}{2}} \cdot r^{\frac{m}{2}} \\
&\quad \cdot S_{\left[\frac{m}{2},2\right]} + v^{m-n-2} \cdot r^{n+2} \cdot S_{[m-n-2,2]} + v^{m-n-1} \cdot r^{n+1} \cdot S_{[m-n-1,2]} \\
&\quad + v^{m-n} \cdot r^n \cdot S_{[m-n,2]} + v^{\frac{2m-n-1}{2}} \cdot r^{\frac{n+1}{2}} \cdot S_{\left[\frac{2m-n-1}{2},2\right]} \\
&\equiv (n+2)^{\frac{m-n-1}{2}} \cdot n^{\frac{n+1}{2}} \cdot (-1)^{\frac{m-n-1}{2}} \cdot 2 \cdot \left[n^{\frac{m}{2}} + (-1)^{\frac{m}{2}} \cdot (n+2)^{\frac{m}{2}}\right] \\
&\quad + (-1) \cdot 2n(n+2) + n(n+2) - 1 + n(n+2) \\
&\equiv (-1)^{\frac{n+1}{2}} \cdot 4 \cdot (n+2)^{\frac{n-1}{2}} \cdot n^{\frac{n+1}{2}} - 1 \pmod 8 \square
\end{aligned}$$

4.2 Computation of V

Lemma 8 *For any $k, 1 \le k \le m-2$,*

$$V_k = \sum_{i=0}^{m-1} x_i^{m-n} \sum_{j=0}^{k} (-1)^j \cdot \frac{1}{(k-j)!} \cdot x_i^{2j} \cdot S_{(k-j,2)}$$

Proof. By lemma 2 and lemma 5,

$$V_k = \sum_{\substack{i \neq j_1, \cdots, j_k \\ j_1 < \cdots < j_k}} x_i^{m-n} x_{j_1}^2 \cdots x_{j_k}^2 = \sum_{i=0}^{m-1} x_i^{m-n} \left(\sum_{\substack{i \neq j_1, \cdots, j_k \\ j_1 < \cdots < j_k}} x_{j_1}^2 \cdots x_{j_k}^2 \right) =$$
$$= \sum_{i=0}^{m-1} x_i^{m-n} \cdot \frac{1}{k!} \cdot U_{k,2} = \sum_{i=0}^{m-1} x_i^{m-n} \sum_{j=0}^{k} (-1)^j \cdot \frac{1}{(k-j)!} \cdot x_i^{2j} \cdot S_{(k-j,2)} \square$$

Using lemma 8 and the values of $S_{(k,2)}$ we have non-zero values of V_k as follows.

k	V_k	k	V_k
$\frac{m-n-3}{2}$	$(-1)^{\frac{m-n-3}{2}} \cdot (2m-2n-3)$	$m-n-3$	$-(m-n-2)$
$\frac{m-n-1}{2}$	$(-1)^{\frac{m-n+1}{2}}$	$m-n-2$	$m-n-2$
$\frac{m}{2}-1$	$(-1)^{\frac{m}{2}-1} \cdot (2m-n-2)$	$m-n-1$	$-(m-n-2)$
$\frac{m}{2}$	$(-1)^{\frac{m}{2}} \cdot n$	$\frac{2m-n-3}{2}$	$(-1)^{\frac{2m-n-3}{2}} \cdot 2\,(m-n-2)$

Lemma 9 $V \equiv -m(2n+1) \pmod 8$

Proof.

$$\begin{aligned}
V &= u \sum_{k=1}^{m-2} v^k r^{m-k-1} V_k \\
&\equiv m(n+2)^{\frac{m-n-3}{2}} \cdot n^{\frac{m+n+1}{2}} \cdot (-1)^{\frac{m-n-3}{2}} \cdot (2m-2n-3) \\
&+ m(n+2)^{\frac{m-n-1}{2}} \cdot n^{\frac{m+n-1}{2}} \cdot (-1)^{\frac{m-n+1}{2}} \\
&+ m(n+2)^{\frac{m}{2}-1} \cdot n^{\frac{m}{2}} \cdot (-1)^{\frac{m}{2}-1} \cdot (2m-n-2) \\
&+ m(n+2)^{\frac{m}{2}} \cdot n^{\frac{m}{2}-1} \cdot (-1)^{\frac{m}{2}} \cdot n \\
&- m(n+2)^{m-n-3} \cdot n^{n+2} \cdot (m-n-2) \\
&+ m(n+2)^{m-n-2} \cdot n^{n+1} \cdot (m-n-2) \\
&- m(n+2)^{m-n-1} \cdot n^{n} \cdot (m-n-2) \\
&+ m(n+2)^{\frac{2m-n-3}{2}} \cdot n^{\frac{n+1}{2}} \cdot (-1)^{\frac{2m-n-3}{2}} \cdot 2 \cdot (m-n-2) \\
&\equiv -m(2n+1) \pmod 8 \square
\end{aligned}$$

4.3 Computation of W

We first determine W_k for each $k, 1 \le k \le m-2$. To do this we introduce another new notation. For fixed different integers $i_1, i_2, 1 \le i_1, i_2 < m$, let

$$Q_k = \sum_{\substack{i_1, i_2 \neq j_1, \cdots, j_k \\ j_l \neq j_t}} x_{j_1}^2 \cdots x_{j_k}^2$$

and put $Q_0 = 1$. We obtain the following lemma by a consideration similar as lemma 5.

Lemma 10 *For any k,*

$$Q_k = \sum_{j=0}^{k} (-1)^j \cdot \frac{k!}{(k-j)!} \cdot x_{i_1}^{2j} \cdot U_{k-j,2}$$

Proof.

$$\begin{aligned}
Q_k &= \sum_{\substack{i_2 \neq j_1, \cdots, j_k \\ j_l \neq j_t}} x_{j_1}^2 \cdots x_{j_k}^2 - k x_{i_1}^2 \sum_{\substack{i_1, i_2 \neq j_1, \cdots, j_{k-1} \\ j_l \neq j_t}} x_{j_1}^2 \cdots x_{j_{k-1}}^2 \\
&= U_{k,2} - k x_{i_1}^2 Q_{k-1} = U_{k,2} - k x_{i_1}^2 \left[U_{k-1,2} - (k-1) x_{i_1}^2 Q_{k-2} \right] \\
&= U_{k,2} - k x_{i_1}^2 U_{k-1,2} + k(k-1) x_{i_1}^{2 \cdot 2} Q_{k-2} = \cdots \\
&= U_{k,2} - k x_{i_1}^2 U_{k-1,2} + k(k-1) x_{i_1}^{2 \cdot 2} U_{k-2,2} + \cdots + (-1)^{k-1} k(k-1) \cdots \\
2 \cdot x_{i_1}^{2(k-1)} \cdot \left[U_{1,2} - x_{i_1}^2 \right] &= \sum_{j=0}^{k} (-1)^j \cdot \frac{k!}{(k-j)!} \cdot x_{i_1}^{2j} \cdot U_{k-j,2} \square
\end{aligned}$$

Using lemma 5 with already computed non-zero values of $S_{(k,2)}$, we get the values of $U_{k,2}$ for any $k \in [0, m-1]$. The result is as follows.

$$\begin{aligned}
&0 \leq k < \frac{m-n-1}{2} \Longrightarrow U_{k,2} = (-1)^k \cdot k! \cdot x_{i_2}^{2k} \\
&\frac{m-n-1}{2} \leq k < \frac{m}{2} \Longrightarrow U_{k,2} = (-1)^k \cdot k! \cdot \left[x_{i_2}^{2k} + 2 x_{i_2}^{2k-(m-n-1)} \right] \\
&\frac{m}{2} \leq k < m-n-2 \Longrightarrow U_{k,2} = (-1)^k \cdot k! \cdot \left[x_{i_2}^{2k} + 2 x_{i_2}^{2k-(m-n-1)} + 2 x_{i_2}^{2k-m)} \right] \\
&U_{m-n-2,2} = -(m-n-2)! \cdot \left[x_{i_2}^{2(m-n-2)} + 2 x_{i_2}^{m-n-3} + 2 x_{i_2}^{m-2n-4)} - 1 \right] \\
&U_{m-n-1,2} = (m-n-1)! \cdot \left[x_{i_2}^{2(m-n-1)} + 2 x_{i_2}^{m-n-1} + 2 x_{i_2}^{m-2n-2)} - x_{i_2}^2 + 1 \right]
\end{aligned}$$

$$\begin{aligned}
m-n \leq k < \frac{2m-n-1}{2} \Longrightarrow U_{k,2} &= (-1)^k \cdot k! \cdot \left[x_{i_2}^{2k} + 2 x_{i_2}^{2k-(m-n-1)} + 2 x_{i_2}^{2k-m} \right] \\
&+ (-1)^{k+1} \cdot k! \cdot \left[x_{i_2}^{2k-2(m-n-2)} + x_{i_2}^{2k-2(m-n-1)} + x_{i_2}^{2k-2(m-n)} \right] \\
\frac{2m-n-1}{2} \leq k < m \Longrightarrow U_{k,2} &= (-1)^k \cdot k! \cdot \left[x_{i_2}^{2k} + 2 x_{i_2}^{2k-(m-n-1)} + 2 x_{i_2}^{2k-m} \right] \\
+ (-1)^{k+1} \cdot k! \cdot \left[x_{i_2}^{2k-2(m-n-2)} + x_{i_2}^{2k-2(m-n-1)} + x_{i_2}^{2k-2(m-n)} - 2 x_{i_2}^{2k-(2m-n-1)} \right]
\end{aligned}$$

Now we find the expression of W_k. By lemma 2, lemma 10 and above equations, we obtain the following for any $k \in [1, m-3]$. Since $U_{k,2}$ depends on the index k, the expression for W_k is also different according to k. For example, if $\frac{m}{2} \leq k < m-n-2$, then W_k is the sum of first 6 terms in the right side of the last equation. We note the non-zero values of W_k for all $k \in [1, m-3]$ in the following table.

k	W_k
$\frac{n-1}{2}$	$(-1)^{\frac{n+1}{2}}\frac{1}{4}(n+1)(2m-n-1)$
n	$\frac{1}{2}m(n+1)$
$\frac{m-n-5}{2}$	$(-1)^{\frac{n-1}{2}}\frac{1}{4}(m-n-3)(3m-3n-5)$
$\frac{m-n-3}{2}$	$(-1)^{\frac{n-1}{2}}\left[\frac{1}{4}(m-n+1)^2-2\right]$
$\frac{m-n-1}{2}$	$(-1)^{\frac{n+1}{2}}\frac{1}{4}(m-n-1)^2$
$\frac{m}{2}-2$	$-\frac{1}{4}(m-2)(3m-2n-4)$
$\frac{m}{2}-1$	$\frac{1}{4}\left(m^2+2mn-2n^2-2m-4n+2\right)$
$\frac{m}{2}$	$\frac{1}{4}m(m-2n-2)$
$\frac{m+n-1}{2}$	$(-1)^{\frac{n+1}{2}}\frac{1}{4}\left(3m^2-6mn+n^2-6m+2n+1\right)$
$\frac{m+2n}{2}$	$\frac{1}{4}m(m-2n-2)$
$m-n-4$	$\frac{1}{2}(m-n-3)(m-n-2)$
$m-n-3$	$-\frac{1}{2}\left(m^2-2mn+n^2-5m+5n+6\right)$
$m-n-2$	$\frac{1}{2}(m-n-2)(m-n-3)$
$\frac{2m-n-5}{2}$	$(-1)^{\frac{n+1}{2}}\left(m^2-2mn+n^2-5m+5n+6\right)$

Now we derive a formula for computation of W modulo 8.

Lemma 11

$$W \equiv \frac{1}{2}m^2(n+1)+(-1)^{\frac{n+1}{2}}\frac{1}{2}m^2(n+2)^{\frac{n+1}{2}}n^{\frac{n+1}{2}}(m+n+3) \pmod 8$$

Proof. It follows from the computation of

$$W = u^2\sum_{k=1}^{m-3} v^k r^{m-k-2}W_k$$

modulo 8 based on the above table. □

4.4 Computation of X, Y, Z

The computations of X, Y, Z are very similar to ones of V, W, so we omit their concrete process but point out only the differences and results.
For any $k, 1 \le k \le m-2$,

$$X_k = \sum_{i=0}^{m-1} x_i \sum_{j=0}^{k}(-1)^j \cdot \frac{1}{(k-j)!}\cdot x_i^{2j}\cdot S_{(k-j,2)}$$

k	X_k	k	X_k
$\frac{m-n-3}{2}$	$(-1)^{\frac{m-n-1}{2}}(m-n-2)$	$m-n-1$	-1
$\frac{m-n-1}{2}$	$(-1)^{\frac{m-n+1}{2}}(m-n)$	$\frac{2m-n-3}{2}$	$(-1)^{\frac{2m-n-3}{2}}(n+2)$
$m-n-2$	-1	$\frac{2m-n-1}{2}$	$(-1)^{\frac{2m-n-1}{2}}n$

Lemma 12 $X \equiv 0 \pmod 8$

For any $k, 1 \le k \le m-2$,

$$\begin{aligned}
Y_k = &\frac{1}{2}(-1)^{k+1}(k+1)\cdot S_{2k+2} + \frac{1}{2}(-1)^k \sum_{j=0}^{k} (S_{2j+1}\cdot S_{2k-2j+1}) \\
&+ (-1)^{k+1}(k - \frac{m-n-1}{2} + 1)\cdot S_{2k-(m-n)+3} \\
&+ (-1)^k \sum_{j=0}^{k-\frac{m-n-1}{2}} \left(S_{2j+1}\cdot S_{2k-2j-(m-n)+2}\right) \\
&+ (-1)^{k+1}(k - \frac{m}{2} + 1)\cdot S_{2k-m+2} \\
&+ (-1)^k \sum_{j=0}^{k-\frac{m}{2}} (S_{2j+1}\cdot S_{2k-2j-m+1}) \\
&+ \frac{1}{2}(-1)^k(k-m+n+3)\cdot S_{2k-2(m-n)+6} \\
&+ \frac{1}{2}(-1)^{k-1} \sum_{j=0}^{k-(m-n-2)} \left(S_{2j+1}\cdot S_{2k-2j-2(m-n-2)+1}\right) \\
&+ \frac{1}{2}(-1)^k(k-m+n+2)\cdot S_{2k-2(m-n)+4} \\
&+ \frac{1}{2}(-1)^{k-1} \sum_{j=0}^{k-(m-n-1)} \left(S_{2j+1}\cdot S_{2k-2j-2(m-n-1)+1}\right) \\
&+ \frac{1}{2}(-1)^k(k-m+n+1)\cdot S_{2k-2(m-n)+2} \\
&+ \frac{1}{2}(-1)^{k-1} \sum_{j=0}^{k-(m-n)} \left(S_{2j+1}\cdot S_{2k-2j-2(m-n)+1}\right) \\
&+ (-1)^{k+1}(k - \frac{2m-n-1}{2} + 1)\cdot S_{2k-(2m-n-1)+2} \\
&+ (-1)^k \sum_{j=0}^{k-\frac{2m-n-1}{2}} \left(S_{2j+1}\cdot S_{2k-2j-(2m-n-1)+1}\right)
\end{aligned}$$

k	Y_k	k	Y_k
$\frac{m-n-3}{2}$	$(-1)^{\frac{m-n+1}{2}}\frac{1}{4}(m-n-1)^2$	$m-n-2$	1
$\frac{m}{2}-1$	$(-1)^{\frac{m}{2}-1}\frac{1}{4}m^2$	$\frac{2m-n-3}{2}$	$(-1)^{\frac{2m-n+1}{2}}\frac{1}{4}(n+1)^2$

Lemma 13 $Y \equiv (-1)^{\frac{n-1}{2}}\frac{1}{2}m(n+1)^2(n+2)^{\frac{n+1}{2}}n^{\frac{n-1}{2}} \pmod 8$

$$
\begin{aligned}
Z_k &= \sum_{i_1 \neq i_2} x_{i_1}^{m-n} x_{i_2} \cdot \frac{1}{k!} \cdot Q_k \\
&= (-1)^{k+1}(k+1) S_{m-n+2k+1} \\
&+ (-1)^k \sum_{j=0}^{k} (S_{m-n+2j} \cdot S_{2k-2j+1}) \\
&+ (-1)^{k+1} \cdot 2 \left(k - \frac{m-n-1}{2} + 1 \right) \cdot S_{2k+2} \\
&+ (-1)^k \cdot 2 \sum_{j=0}^{k-\frac{m-n-1}{2}} \left(S_{m-n+2j} \cdot S_{2k-2j-(m-n-1)+1} \right) \\
&+ (-1)^{k+1} \cdot 2 \left(k - \frac{m}{2} + 1 \right) \cdot S_{2k-n+1} \\
&+ (-1)^k \cdot 2 \sum_{j=0}^{k-\frac{m}{2}} (S_{m-n+2j} \cdot S_{2k-2j-m+1}) \\
&+ (-1)^k (k-m+n+3) \cdot S_{2k-m+n+5} \\
&+ (-1)^{k-1} \sum_{j=0}^{k-(m-n-2)} \left(S_{m-n+2j} \cdot S_{2k-2j-2(m-n-2)+1} \right) \\
&+ (-1)^k (k-m+n+2) \cdot S_{2k-m+n+3} \\
&+ (-1)^{k-1} \sum_{j=0}^{k-(m-n-1)} \left(S_{m-n+2j} \cdot S_{2k-2j-2(m-n-1)+1} \right) \\
&+ (-1)^k (k-m+n+1) \cdot S_{2k-m+n+1} \\
&+ (-1)^{k-1} \sum_{j=0}^{k-(m-n)} \left(S_{m-n+2j} \cdot S_{2k-2j-2(m-n)+1} \right) \\
&+ (-1)^{k+1} \cdot 2 \left(k - \frac{2m-n-1}{2} + 1 \right) \cdot S_{2k-m+2} \\
&+ (-1)^k \cdot 2 \sum_{j=0}^{k-\frac{2m-n-1}{2}} \left(S_{m-n+2j} \cdot S_{2k-2j-(2m-n-1)+1} \right)
\end{aligned}
$$

k	Z_k
$\frac{n-1}{2}$	$(-1)^{\frac{n-1}{2}} \frac{1}{2} m(n+1)$
$\frac{m-n-5}{2}$	$(-1)^{\frac{n+1}{2}} \frac{1}{2}(m-n-3)(m-n-2)$
$\frac{m-n-3}{2}$	$(-1)^{\frac{n-1}{2}} \frac{1}{2}\left[(m-n)^2 - 2(m-n) + 3\right]$
$\frac{m-n-1}{2}$	$(-1)^{\frac{n-1}{2}} \frac{1}{2}(m-n)(m-n-1)$
$\frac{m}{2} - 1$	$-\frac{1}{2} m(2m-3n-3)$
$\frac{m+n-1}{2}$	$(-1)^{\frac{n-1}{2}} \frac{1}{2} m(m-n-1)$
$m-n-3$	$m-n-2$
$m-n-2$	$m-n-2$
$\frac{2m-n-5}{2}$	$(-1)^{\frac{n+1}{2}}(mn - n^2 + 2m - 4n - 4)$
$\frac{2m-n-3}{2}$	$(-1)^{\frac{n-1}{2}} 2n(m-n-2)$

Lemma 14 $Z \equiv 0 \pmod 8$

Now using above lemmas we compute the resultant $R(F,G)$ modulo 8 in case of m even, not dividable by 4 and n odd.

Lemma 15 *Under the above assumption, it satisfies*

$$R(F,G) \equiv 1 - m - 2mn + \frac{1}{2}m^2(n+1) + (-1)^{\frac{n+1}{2}} m^2 n^{\frac{n+1}{2}} (n+2)^{\frac{n+1}{2}} \pmod 8 \tag{10}$$

Proof.

$$\begin{aligned} R(F,G) \equiv\ & v^m + r^m + uv^{m-1} \cdot S_{m-n-2} + ur^{m-1} \cdot S_{m-n} + v^{m-1}w \cdot S_{-1} + wr^{m-1} \cdot S_1 + \\ & + u^2 v^{m-2} \cdot S_{[2,m-n-2]} + u^2 r^{m-2} \cdot S_{[2,m-n]} + v^{m-2}w^2 \cdot S_{[2,-1]} + w^2 r^{m-2} \cdot S_{[2,1]} \\ & + uv^{m-2}w \cdot S_{m-n-2,-1} + uwr^{m-2} \cdot S_{m-n,1} + S + V + W + X + Y + Z \pmod 8. \end{aligned}$$

Since we assumed that $n > 6$ and $m > 6(n-2)$, $S_{-1} = S_1 = S_{[2,-1]} = S_{[2,1]} = 0$. And by lemma 2

$$\begin{aligned} S_{m-n-2,-1} &= S_{m-n-2} \cdot S_{-1} - S_{m-n-3} = 0 \\ S_{m-n,1} &= S_{m-n} \cdot S_1 - S_{m-n+1} = 0 \end{aligned}$$

Thus we get

$$\begin{aligned} R(F,G) \equiv\ & 2 + m(n+2) \cdot S_{m-n-2} + mn \cdot S_{m-n} + \frac{1}{2}m^2 \left(S_{m-n-2}^2 - S_{2(m-n-2)}\right) \\ & + \frac{1}{2}m^2 \left(S_{m-n}^2 - S_{2(m-n)}\right) + S + V + W + X + Y + Z \pmod 8 \end{aligned}$$

The assertion is followed by substituting the corresponding values to the above equation. □

Theorem 5 *If m is even, not divided by 4, and n is odd, then the pentanomial (9) has an even number of the irreducible factors over $\mathbf{F}_2$ if and only if one of the following conditions holds* :

(1) $m \equiv 2 \pmod 8$ *and* $n \equiv 3, 7 \pmod 8$
(2) $m \equiv 6 \pmod 8$ *and* $n \equiv 1, 5 \pmod 8$

Proof. The discriminant of F is as follows.

$$\begin{aligned} D(F) &= (-1)^{m(m-1)/2} \cdot R(F,G) \equiv \\ &\equiv -\left(1 - m - 2mn + \frac{1}{2}m^2(n+1) + (-1)^{\frac{n+1}{2}} m^2 n^{\frac{n+1}{2}} (n+2)^{\frac{n+1}{2}}\right) \\ &\quad \pmod 8 \end{aligned}$$

Thus we search all possible cases, namly

$$\begin{aligned} m \equiv 2 \pmod 8&, \\ n \equiv 1 \pmod 8 &\Longrightarrow D(F) \equiv 5 \pmod 8 \\ n \equiv 3 \pmod 8 &\Longrightarrow D(F) \equiv 1 \pmod 8 \\ n \equiv 5 \pmod 8 &\Longrightarrow D(F) \equiv 5 \pmod 8 \\ n \equiv 7 \pmod 8 &\Longrightarrow D(F) \equiv 1 \pmod 8 \end{aligned}$$

$$
\begin{aligned}
&m \equiv 6 \pmod 8, \\
&\quad n \equiv 1 \pmod 8 \Longrightarrow D(F) \equiv 1 \pmod 8 \\
&\quad n \equiv 3 \pmod 8 \Longrightarrow D(F) \equiv 5 \pmod 8 \\
&\quad n \equiv 5 \pmod 8 \Longrightarrow D(F) \equiv 1 \pmod 8 \\
&\quad n \equiv 7 \pmod 8 \Longrightarrow D(F) \equiv 5 \pmod 8
\end{aligned}
$$

Therefore we obtain the result of the theorem. □

Finally we consider the case of m, multiple of 4. In this case we can see directly $W \equiv Z \equiv 0 \pmod 8$. In the same manner we compute the discriminant of F but we omit details and scribe only the results.

$$
\begin{aligned}
&S \equiv 3 + 4n + (-1)^{\frac{n+1}{2}} 4(2n+1)^{\frac{n+1}{2}} \pmod 8 \\
&V \equiv m \pmod 8 \\
&X \equiv 0 \pmod 8 \\
&Y \equiv 6(n+1) \pmod 8
\end{aligned}
$$

$$
\begin{aligned}
R(F,G) &\equiv 2 - m(n+2)(m-n-2) - mn(m-n) + S + V + Y \equiv \\
&\equiv 3 + 2n + m + (-1)^{\frac{n+1}{2}} 4(2n+1)^{\frac{n+1}{2}} \pmod 8 \qquad (11)
\end{aligned}
$$

Since m is a multiple of 4, $D(F) = (-1)^{m(m-1)/2} \cdot R(F,G) = R(F,G)$, so we have the following theorem.

Theorem 6 *If m is dividable by 4, and n is odd, then the pentanomial (9) has an even number of the irreducible factors over $\mathbf{F}_2$ if and only if one of the following conditions holds* :

(1) $m \equiv 0 \pmod 8$ *and* $n \equiv 1, 5 \pmod 8$

(2) $m \equiv 4 \pmod 8$ *and* $n \equiv 3, 7 \pmod 8$

From theorem 5 and theorem 6 we obtain the following corollary.

Corollary 3 *Let m be even and n be odd and suppose that the pentanomial (9) is irreducible over $\mathbf{F}_2$.*

(1) *If* $n \equiv 1, 5 \pmod 8$, *then* $m \equiv 2, 4 \pmod 8$

(2) *If* $n \equiv 3, 7 \pmod 8$, *then* $m \equiv 0, 6 \pmod 8$

Note that if f is a polynomial over $\mathbf{F}_2$ with no repeated root and F is its monic lift to $\mathbf{Z}[x]$, then $D(F) \equiv 1$ or $5 \pmod 8$ by Stickelberger's theorem.[9] As we see from the proofs of theorem 3,4,5 and 6, the discriminant of the pentanomial $F(x) \in \mathbf{Z}[x]$ is always congruent to 1 or 5 modulo 8. Since $D(f) \equiv D(F) \pmod 8$, this shows that type II pentanomials of even degree have no repeated root.

5 Conclusion

We have determined the parity of the number of irreducible factors for the type II pentanomials of even degrees using the Stickelberger-Swan theorem. Our consideration is similar with one in (1) but the computation is more complex. It will be published elsewhere some results for type II pentanomials of odd degrees and type I pentanomials.

References

[1] O.Ahmadi and A.Menezes, Irreducible polynomials over maximum weight, Utilitas Mathematica, 72(2007), 111-123

[2] O.Ahmadi and A.Menezes, On the number of trace-one elements in polynomial bases for $\mathbf{F}_{2^n}$, Designs, Codes and Cryptography, 37(2005), 493-507

[3] 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, 14(2008), 124-131

[4] A.Bluher, A Swan-like theorem, Finite Fields and Their Applications, 12(2006), 128-138

[5] A.Hales and D.Newhart, Swan's theorem for binary tetranomials, Finite Fields and Their Applications, 12(2006), 301-311

[6] R.Lidl and H.Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1997

[7] K.V.Mangipudi and R.S. Katti, Montgomery multiplier for a class of special irreducible pentanomials, Preprint, 2004

[8] F.Rodriguez-Henriquez and C.K. Koc, Parallel multipliers based on special irreducible pentanomials, IEEE Transactions on Computers, 52(2003), 1535-1542

[9] R.G.Swan, Factorization of polynomials over finite fields", Pacific Journal of Mathematics,12(1962), 1099-1106