International Mathematical Forum, 2, 2007, no. 31, 1507 - 1524

A Characterization for the Reducibility of Some Self-reciprocal Binary Pentanomials

Gerardo Vega

Dirección General de Servicios de Cómputo Académico
Universidad Nacional Autónoma de México
04510 México D.F., Mexico
gerardov@servidor.unam.mx

Abstract

It is well known that a characterization for the irreducibility of self-reciprocal binary pentanomials does not exist [1, 4]. In this work we divide the self-reciprocal binary pentanomials into four big families, in such a way that all members of one of these families are clearly reducible. Using the Berlekamp Algorithm for the factorization of binary polynomials [2], we prove that all members of a second family are also reducible. More specifically, we present a construction through which it is possible to associate, to each one of the pentanomials in this family, a binary symmetric singular submatrix. As we will see, all the nullities of these submatrices are always odd numbers. This, as we will also see, implies that all pentanomials, in this second family, have an even number of irreducible polynomial factors (and for this reason, all of them are reducible).

Mathematics Subject Classification: 11T06

Keywords: Self-reciprocal binary pentanomials, Berlekamp Algorithm and binary polynomials

1 Introduction

Let u and v be two integers greater than 0 and $u < v$, then all the self-reciprocal binary pentanomials given by

$$1 + x^u + x^v + x^{2v-u} + x^{2v} \ ,$$

can be classified into 4 types:

Type 1: u is an even number and v is an even number,
Type 2: u is an even number and v is an odd number,
Type 3: u is an odd number and v is an even number,
Type 4: u is an odd number and v is an odd number.

Clearly, all self-reciprocal binary pentanomials of Type 1 are reducible. The main goal of this work is to show that all of Type 2 are also reducible. More precisely, if $P(x)$ is a self-reciprocal binary pentanomial of Type 2, then $(P(x), P'(x)) = 1$, and thus, we can use the Berlekamp Algorithm in order to obtain the irreducible factors of $P(x)$. With this algorithm, the irreducible factors of $P(x)$ are obtained via the null space of a singular matrix constructed using the polynomial $P(x)$. In fact, the dimension of the null space of this matrix corresponds to the number of distinct irreducible factors of $P(x)$. Through a specific construction, we will show that we can associate an equivalent matrix to this matrix, in such a way, that the nullity of the original matrix will be given by the nullity of a well defined symmetric submatrix that lies within the equivalent one. Due to some relevant properties of these symmetric submatrices, we will conclude that their nullities will always be odd numbers. This, as we will see, implies that all self-reciprocal binary pentanomials of Type 2 have an even number of irreducible polynomial factors.

This work is organized as follows: in Section 2 we present the specific construction, which allows us to associate a binary submatrix to each self-reciprocal binary pentanomial of Type 2. In Section 3 we show that all of these submatrices are symmetric, whereas in Section 4 we present some other relevant properties of these submatrices. The aforementioned result is presented in Section 5. Finally, Section 6 is devoted to conclusions.

2 The Construction

Let $P(x)$ be a binary polynomial of positive degree n, such that $(P(x), P'(x)) = 1$. Using $P(x)$ we set n binary polynomials of degree less than n, given by $R_i(x) = \sum_{j=0}^{n-1} b_{i,j}x^j = x^i + x^{2i} \mathrm{mod} P(x)$, for $i = 0, 1, 2, \ldots, n-1$. The Berlekamp Algorithm [2, Ch. 4, pp. 132-137] shows us that the number of irreducible factors of $P(x)$ will corresponds to the dimension of the null space of the $n \times n$ matrix given by $B = \{b_{i,j}\}$. Let us note that each row vector $R_i = (b_{i,0}, b_{i,1}, \ldots, b_{i,n-1})$ of B is determined by its corresponding polynomial

$R_i(x)$. Due to this relationship, we will refer to these polynomials as *Row Polynomials of* B. Now, if $P(x)$ is a self-reciprocal binary pentanomial of Type 2, then we have that u is an even positive number, v is an odd positive number with $u < v$ and $n = 2v$. Besides, the row polynomials are given by

$$\begin{aligned} R_i(x) &= x^i + x^{2i} \\ R_{v+i}(x) &= \sum_{j=0}^{\lfloor \frac{2i}{u} \rfloor} x^{2i-uj} P(x) + \sum_{j=0}^{\lfloor \frac{2i-v}{2u} \rfloor} x^{2i-v-2uj} P(x) + \\ &\quad \delta(2i \geq n-u) x^{2i-(n-u)} P(x) + x^{v+i} + x^{2(v+i)} \ , \end{aligned} \tag{1}$$

where $i = 0, 1, 2, \ldots, v-1$ and $\delta(\cdot)$ is the $\{0,1\}$-valued function such that its value is one iff its argument is true. Note that all the row polynomials have, indeed, degree less than n. For example, if $u = 4$ and $v = 5$, then $P(x) = 1 + x^4 + x^5 + x^6 + x^{10}$ and $R_8(x) = (x^6 + x^2)P(x) + xP(x) + P(x) + x^8 + x^{16} = 1 + x + x^2 + x^4$.

Now, we are going to apply some specific row and column operations on B, but first, we will start by fixing some notation and giving some definitions. The integers u, v and n, the polynomials $R_i(x)$, the vectors R_i and the $n \times n$ matrix B, are as before. Since v is an odd integer greater that 1, we fix $t = (v-1)/2$. We define the functions $l, \lambda : \mathbb{Z} \to \mathbb{Z}$ by

$$l(i) = \max\{k \in \mathbb{Z} \mid \frac{i}{2^k} \in \mathbb{Z}\} \ , \qquad \lambda(i) = \frac{i}{2^{l(i)}} \ .$$

For each $a = 1, 2, \ldots, t$, we denote $t_a = t + a$, $l_a = l(t+a)$ and $\lambda_a = \lambda(t+a)$. One verifies at once that for any integer b, with $1 \leq b \leq t$, we have $\lambda_a = \lambda_b$ iff $a = b$. For such values of a, J_a^u, denotes the integer given by

$$J_a^u = \begin{cases} 0 & \text{if } \lambda_a > u \\ \max\{k \in \mathbb{Z} \mid 2^k \lambda_a \leq u\} & \text{otherwise} \end{cases} \ .$$

With these definitions and notations, we apply row operations on B.

Algorithm 1 *This algorithm applies a set of specific row operations on the last* t *rows of matrix* B*. Here, the left arrow, "*$\leftarrow$*", between two polynomials, means that the polynomial on the right hand side must be added to the polynomial on the left hand side.*

for $a = t$ **downto** 1 **do**

for $j = 0$ **to** $J_a^u - 1$ **do** $R_{v+t_a}(x) \leftarrow R_{v+2^j\lambda_a}(x)$

for $j = J_a^u$ **to** l_a **do**

if $j < l_a$ **then** $R_{v+t_a}(x) \leftarrow R_{v+2^j\lambda_a}(x)$
$R_{v+t_a}(x) \leftarrow R_{v+2^j\lambda_a-u}(x)$

end for
if $\lambda_a \leq u$ **then** $R_{v+t_a}(x) \leftarrow R_{v+2^{J_a^u}\lambda_a-u}(x)$

end for
$R_{n-(u/2)}(x) \leftarrow R_v(x)$

As a result of Algorithm 1, we obtain a matrix equivalent to B, which we will denote by $\tilde{B}$. Its row polynomials, $\tilde{R}_i(x)$, will be as follows

$$\tilde{R}_i(x) = R_i(x) \ , \tag{2}$$

for $i = 0, 1, \ldots, v + t$, and for $a = 1, 2, \ldots, t$, we have

$$\begin{aligned} \tilde{R}_{v+t_a}(x) &= \sum_{j=0}^{J_a^u-1} R_{v+2^j\lambda_a}(x) + \sum_{j=J_a^u}^{l_a} (R_{v+2^j\lambda_a}(x) + R_{v+2^j\lambda_a-u}(x)) + \\ &\quad \delta(\lambda_a \leq u) R_{v+2^{J_a^u}\lambda_a-u}(x) + \delta(v + t_a = n - (u/2)) R_v(x) \ . \end{aligned} \tag{3}$$

Rearranging sums

$$\begin{aligned} \tilde{R}_{v+t_a}(x) &= \sum_{j=0}^{J_a^u-1} R_{v+2^j\lambda_a}(x) + \delta(\lambda_a \leq u) R_{v+2^{J_a^u}\lambda_a}(x) + \\ &\quad \sum_{j=J_a^u+\delta(\lambda_a\leq u)}^{l_a} (R_{v+2^j\lambda_a}(x) + R_{v+2^j\lambda_a-u}(x)) + \\ &\quad \delta(2t_a = n - u) R_v(x) \ . \end{aligned}$$

Since $0 \leq j < J_a^u$ for the first summation, then $\lfloor 2^{j+1}\lambda_a/u \rfloor = \delta((j + 1 = J_a^u)$ and $(2^{J_a^u} = u))$ and $2^{j+1}\lambda_a \leq u < v < n - u$. Thus, by using (1), we have

$$\begin{aligned} \sum_{j=0}^{J_a^u-1} R_{v+2^j\lambda_a}(x) &= \sum_{j=0}^{J_a^u-1} (x^{2^{j+1}\lambda_a} P(x) + x^{v+2^j\lambda_a} + x^{n+2^{j+1}\lambda_a}) + \\ &\quad \delta(2^{J_a^u}\lambda_a = u) P(x) \ . \end{aligned} \tag{4}$$

Now, if $\lambda_a \leq u$, then $\lfloor 2^{J_a^u+1}\lambda_a/u \rfloor = 1 + \delta(2^{J_a^u} = u)$ and $\lfloor (2^{J_a^u+1}\lambda_a - v)/2u \rfloor \leq 0$. Besides, since $v < 2t_a \leq 4t < n$, it follows that if $2^{J_a^u+1}\lambda_a > v$ or $2^{J_a^u+1}\lambda_a \geq n-u > v$, then $J_a^u = l_a$ and $2^{J_a^u+1}\lambda_a = 2t_a$. Thus, if $\lambda_a \leq u$, we can write

$$\begin{aligned} R_{v+2^{J_a^u}\lambda_a}(x) &= (x^{2^{J_a^u+1}\lambda_a} + x^{2^{J_a^u+1}\lambda_a - u} + \delta(2^{J_a^u}\lambda_a = u))P(x) + \\ &\quad \delta(2^{J_a^u+1}\lambda_a > v)x^{2t_a - v}P(x) + \\ &\quad \delta(2^{J_a^u+1}\lambda_a \geq n-u)x^{2t_a-(n-u)}P(x) + \\ &\quad x^{v+2^{J_a^u}\lambda_a} + x^{n+2^{J_a^u+1}\lambda_a} . \end{aligned} \tag{5}$$

In the case when $u \leq i < v$, we have

$$\begin{aligned} \sum_{j=0}^{\lfloor \frac{2i}{u} \rfloor} x^{2i-uj}P(x) &= (x^{2i} + x^{2i-u})P(x) + \sum_{j=0}^{\lfloor \frac{2(i-u)}{u} \rfloor} x^{2(i-u)-uj}P(x) , \\ \sum_{j=0}^{\lfloor \frac{2i-v}{2u} \rfloor} x^{2i-v-2uj}P(x) &= \delta(2i > v)x^{2i-v}P(x) + \sum_{j=0}^{\lfloor \frac{2(i-u)-v}{2u} \rfloor} x^{2(i-u)-v-2uj}P(x) , \end{aligned}$$

and since $2(i-u) < n-u$, for such values of i, then

$$\begin{aligned} R_{v+i}(x) + R_{v+i-u}(x) &= (x^{2i} + x^{2i-u} + \delta(2i > v)x^{2i-v})P(x) + \\ &\quad \delta(2i \geq n-u)x^{2i-(n-u)}P(x) + \\ &\quad x^{v+i} + x^{n+2i} + x^{v+i-u} + x^{n+2i-2u} . \end{aligned}$$

Now, note that if $J_a^u < j \leq l_a$ or, if $J_a^u \leq j \leq l_a$ and $\lambda_a > u$, then $u < 2^j\lambda_a \leq 2t < v$. Besides $2^{j+1}\lambda_a > v \Leftrightarrow j = l_a$ and $2^{j+1}\lambda_a \geq n-u > v \Rightarrow j = l_a$. Therefore

$$\begin{aligned} \sum_{j=J_a^u+\delta(\lambda_a \leq u)}^{l_a} R_{v+2^j\lambda_a}(x) + R_{v+2^j\lambda_a-u}(x) &= \sum_{j=J_a^u+\delta(\lambda_a \leq u)}^{l_a} ((x^{2^{j+1}\lambda_a} + x^{2^{j+1}\lambda_a-u})P(x) + \\ &\qquad x^{v+2^j\lambda_a} + x^{n+2^{j+1}\lambda_a} + \\ &\qquad x^{v+2^j\lambda_a-u} + x^{n+2^{j+1}\lambda_a-2u}) + \\ &\quad x^{2t_a-v}P(x) + \\ &\quad \delta(2t_a \geq n-u)x^{2t_a-(n-u)}P(x) . \end{aligned} \tag{6}$$

Regrouping (4), (5) and (6)

$$\begin{aligned}\tilde{R}_{v+t_a}(x) &= \sum_{j=0}^{J_a^u-1}(x^{2^{j+1}\lambda_a}P(x)+x^{v+2^j\lambda_a}+x^{n+2^{j+1}\lambda_a})+\\ &\quad \sum_{j=J_a^u}^{l_a}((x^{2^{j+1}\lambda_a}+x^{2^{j+1}\lambda_a-u})P(x)+x^{v+2^j\lambda_a}+\\ &\quad\quad x^{n+2^{j+1}\lambda_a}+x^{v+2^j\lambda_a-u}+x^{n+2^{j+1}\lambda_a-2u})+\\ &\quad \delta(\lambda_a\leq u)(x^{v+2^{J_a^u}\lambda_a-u}+x^{n+2^{J_a^u+1}\lambda_a-2u})+x^{2t_a-v}P(x)+\\ &\quad \delta(2t_a\geq n-u)x^{2t_a-(n-u)}P(x)+\delta(2t_a=n-u)R_v\ .\end{aligned}$$

But $P(x)=1+x^u+x^v+x^{n-u}+x^n$, so the first summation in the previous equation is equal to

$$x^{v+\lambda_a}+x^{v+2^{J_a^u}\lambda_a}+\sum_{j=0}^{J_a^u-1}x^{2^{j+1}\lambda_a}(1+x^u+x^{n-u})\ ,$$

whereas the second one can be replaced by

$$x^{v+2^{J_a^u}\lambda_a}+x^{v+2t_a}+x^{v+2^{J_a^u}\lambda_a-u}+x^{v+2t_a-u}+\sum_{j=J_a^u}^{l_a}x^{2^{j+1}\lambda_a}(x^{-u}+x^u)\ .$$

Besides,

$$\begin{aligned}x^{2t_a-v}P(x) &= x^{2t_a-v}+x^{2t_a-v+u}+x^{2t_a}+x^{2t_a+v-u}+x^{2t_a+v}\\ R_v(x) &= P(x)+x^v+x^n\ .\end{aligned}$$

Putting all together, considering that $2t_a-v=2a-1$, we have

$$\begin{aligned}\tilde{R}_{v+t_a}(x) &= x^{2a-1}(1+x^u+x^v)+x^{m_a^u(2^{J_a^u}\lambda_a-u+v)}+x^{v+\lambda_a}+\\ &\quad \sum_{j=0}^{J_a^u-1}x^{2^{j+1}\lambda_a}(1+x^u+x^{n-u})+\\ &\quad \sum_{j=J_a^u}^{l_a}x^{2^{j+1}\lambda_a}(x^{-u}+x^u)+\delta(2t_a=n-u)(x^v+x^n)+\\ &\quad \delta(2t_a>n-u)x^{2t_a-n+u}(1+x^u+x^v+x^{n-u}+x^n)\ , \qquad (7)\end{aligned}$$

where $m_a^u = 1 + \delta(\lambda_a \leq u)$. Note that if $\lambda_a > u$, then $\lambda_a - u + v$ is an even number and $v < \lambda_a - u + v < n - u$ (since $\lambda_a \leq t_a < v$). On the other hand, if $\lambda_a \leq u$, then $v < n - u < 2(2^{J_a^u}\lambda_a - u + v) \leq n$ (since $-u/2 < 2^{J_a^u}\lambda_a - u \leq 0$). Thus, in any case we have that $m_a^u(2^{J_a^u}\lambda_a - u + v)$ is an even number greater than v and less than or equal to n. Clearly $v + 2a - 1$ and $v + \lambda_a$ are even numbers greater than v and less than n. Also observe that $2a - 1 + u = v \Leftrightarrow 2t_a = n - u$ and $2a - 1 + u > v \Leftrightarrow 2t_a > n - u$, and since $2a - 1 + u = (2t_a - n + u) + v$, we may conclude that the monomial x^{2a-1+u} will be present in the reduction of the row polynomial $\tilde{R}_{v+t_a}(x)$ iff $2a - 1 + u < v$. Now, since $2a - 1 < v$ for all $a = 1, 2, \ldots, t$, this implies that all monomials in the reduction of $\tilde{R}_{v+t_a}(x)$ will have an even degree, if such a degree is greater than $v - 1$. Besides, through a direct inspection, we can see that the constant monomial 1 does not appear in $\tilde{R}_{v+t_a}(x)$.

Now, if $i = 0, 1, \ldots, t$, then $2i - v < 0$ and $2i < n - u$. Hence, for all such values of i, we have

$$R_{v+i}(x) \;=\; \sum_{j=0}^{\lfloor \frac{2i}{u} \rfloor} x^{2i-uj} P(x) + x^{v+i} + x^{2(v+i)} \; .$$

But x^v is the only monomial of odd degree in $P(x)$, so if $a = 1, 2, \ldots, t$, then the monomial of maximum odd degree in $R_{v+a}(x)$ (or $\tilde{R}_{v+a}(x)$), is x^{2a+v}. Particularly, for $R_{v+t}(x)$, such a monomial is $x^{2t+v} = x^{n-1}$. Since $n - 1 > 2a' + v$, for all $a' = 1, 2, \ldots, t - 1$, then $\tilde{R}_{v+t}(x)$ is the only one row polynomial that contains x^{n-1}. This means that we can apply column operations on $\tilde{B}$, in such a way, that we obtain a new equivalent matrix, which we will continue denoting by $\tilde{B}$ in order to simplify the notation, where $\tilde{R}_{v+t}(x) = x^{n-1}$. After these, if $t > 1$, then the monomial x^{n-3} will be present only in the row polynomial $\tilde{R}_{v+t-1}(x)$ and hence, doing as before, such a row polynomial can be replaced by x^{n-3}. We can continue with this procedure until the row polynomial $\tilde{R}_{v+1}(x)$ is replaced by x^{2+v}. Since the row polynomial $R_v(x)$ is the only one that has the constant monomial 1, then such a row polynomial can be replaced by 1. As result of this column operations, the first $n - t$ row polynomials of $\tilde{B}$ are as follows

$$\begin{aligned} \tilde{R}_0(x) &= 0, \qquad \tilde{R}_i(x) = x^i + x^{2i} \qquad \text{for } i = 1, 2, \ldots, v - 1 \; , \\ \tilde{R}_v(x) &= 1, \quad \tilde{R}_{v+a}(x) = x^{2a+v} \qquad \text{for } a = 1, 2, \ldots, t \; , \end{aligned} \tag{8}$$

whereas the last t are as in (7). In order to simplify the row polynomials $\tilde{R}_i(x)$, for $i = 1, 2, \ldots, v - 1$, we add, for such values and for such ordering of i, the

i-th column of $\tilde{B}$, to its $2i$-th column. With this operation we have $\tilde{R}_i(x) = x^i$, for $i = 1, 2, \ldots, v-1$, whereas the other row polynomials in (8) stay without changes. For each $i = 1, 2, \ldots, v-1$, we can now apply row operations, using the new version of $\tilde{R}_i(x)$, in order to delete the monomial x^i from the last t row polynomials: $\tilde{R}_{v+t_a}(x)$, with $a = 1, 2, \ldots, t$. As a result of the application of this new set of row and column operations, the $\tilde{B}$ matrix is as follows

$$\begin{array}{rcl} \tilde{R}_0(x) & = & 0, \quad \tilde{R}_i(x) = x^i \qquad \text{for } i = 1, 2, \ldots, v-1 \ , \\ \tilde{R}_v(x) & = & 1, \quad \tilde{R}_{v+a}(x) = x^{2a+v} \qquad \text{for } a = 1, 2, \ldots, t \ , \end{array} \tag{9}$$

for the first $n - t$ row polynomials of $\tilde{B}$, and

$$\begin{array}{rcl} \tilde{R}_{v+t_a}(x) & = & x^{\gamma_v(2a-1)} + x^{\gamma_v(2a-1+u)} + x^{2t_a} + x^{m_a^u(2^{J_a^u}\lambda_a - u + v)} + x^{v+\lambda_a} + \\ & & \sum_{j=0}^{J_a^u - 1} (x^{2t_a} + x^{\gamma_v(2^{j+1}\lambda_a + u)} + x^{2^{j+1}\lambda_a + n - u}) + \\ & & \sum_{j=J_a^u}^{l_a} (x^{\gamma_v(2^{j+1}\lambda_a - u)} + x^{\gamma_v(2^{j+1}\lambda_a + u)}) + \delta(2t_a = n-u)(x^v + x^n) + \\ & & \delta(2t_a > n-u)(x^{\gamma_v(2t_a - n + u)} + x^{\gamma_v(2t_a - n + 2u)} + \\ & & \qquad x^{2a-1+u} + x^{2t_a} + x^{2t_a + u}) \ , \end{array} \tag{10}$$

for the last t ones, and where γ_v is an integer function defined for all positive integers greater than 0, which is given by

$$\gamma_v(i) = \begin{cases} i & \text{if } i \geq 2v \\ \max\{k \in \mathbb{Z} \mid k < 2v \text{ and } k = 2^s i \text{ for some } s \in \mathbb{Z}\} & \text{otherwise} \end{cases} .$$

The only difference between (7) and (10), is just the γ_v function, which appears as a result of the last column operations. Note that $\gamma_v(i) = i$, for all $i \geq v$ (not $2v$). As an example of the construction presented here, we use the pentanomial $P(x) = 1 + x^4 + x^7 + x^{10} + x^{14}$. For this, Figure 1(a) shows the matrix that is obtained by (1), whereas Figure 1(b), shows the one that is obtained after applying Algorithm 1 (or through (2) and (3), or (2) and (7)). On the other hand, the first matrix in Figure 2 corresponds to the one that is obtained by (8) and (7), whereas the second one, is the one that is obtained by (9) and (10).

As can be seen from (9) and (10) (also see Figure 2(b)), the rows $\tilde{R}_i$, with $i = 1, 2, \ldots, v + t$ are linear independent, and linear independent with respect

(a)
$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
1&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&1&0&1&1&0&0&1&0&0\\
1&0&0&0&0&0&0&1&1&1&1&1&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&1&1&0\\
1&1&0&0&0&1&0&1&1&0&1&1&1&0&0\\
1&0&1&1&1&0&0&0&0&1&0&0&0&0&0\\
1&0&1&0&0&1&1&1&0&0&1&1&0&1&0
\end{bmatrix}$$

(b)
$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
1&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&1&0&1&1&0&0&1&0&0\\
1&0&0&0&0&0&0&1&1&1&1&1&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&1&1&0\\
0&1&1&0&0&1&1&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&1&0&1&0&1&0&0\\
0&0&0&0&0&1&1&0&1&0&0&0&1&0&0
\end{bmatrix}$$

Figure 1: (a) Matrix obtained by (1). (b) Matrix obtained by (2) and (7). In both cases we are using the pentanomial $P(x) = 1 + x^4 + x^7 + x^{10} + x^{14}$.

to the last t rows of $\tilde{B}$. This means that a self-reciprocal binary pentanomial of Type 2 will be reducible, iff the submatrix obtained from $\tilde{B}$, by intersecting its last t rows with its last t columns with an even position (*ie*, if we denote by $\tilde{C}_i$, with $i = 0, 1, \ldots, n-1$, the n columns of $\tilde{B}$, then we are referring to the columns: $\tilde{C}_{v+1}, \tilde{C}_{v+3}, \ldots, \tilde{C}_{n-2}$) is singular. For Figure 2(b), such a submatrix is

$$\begin{bmatrix} 1&1&1\\ 1&1&1\\ 1&1&0 \end{bmatrix}.$$

In the next section, we will show that the symmetric shape of the previous submatrix is something more than a fortunate choice.

3 All these Submatrices are Symmetric

To avoid repetition, from now on we will denote by $\mathcal{B}$ the $t \times t$ submatrix that is obtained by intersecting the last t rows with the last t columns, with an even position, of the matrix $\tilde{B}$ given by (9) and (10). In order to prove the symmetric shape of $\mathcal{B}$, we must show that for any pair of integers a and

(a)
$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&1&0&0&1&1&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&1&0&1&0&1&0&0\\
0&0&0&0&0&1&1&0&1&0&0&0&1&0&0
\end{bmatrix}$$

(b)
$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&1&0&1&0&0&0&0
\end{bmatrix}$$

Figure 2: (a) Matrix obtained by (8) and (7). (b) Matrix obtained by (9) and (10). Both cases uses the pentanomial $P(x) = 1 + x^4 + x^7 + x^{10} + x^{14}$.

b, with $1 \leq a, b \leq t$, the monomial x^{2t_b} is in the row polynomial $\tilde{R}_{v+t_a}(x)$ iff the monomial x^{2t_a} is in $\tilde{R}_{v+t_b}(x)$. It must be observed that monomial x^{2t_a}, in $\tilde{R}_{v+t_a}(x)$, determines the diagonal element for the a-th row of submatrix $\mathcal{B}$.

We start our analysis by considering the monomials $x^{\gamma_v(2a-1)}$ and $x^{v+\lambda_a}$.

Lemma 1 *Let a and b be as before, then $\gamma_v(2a-1) = 2t_b$ iff $v + \lambda_b = 2t_a$.*

Proof: Since $2a-1$ and λ_b are odd numbers, then $\gamma_v(2a-1) = 2t_b \Leftrightarrow 2a-1 = \lambda_b \Leftrightarrow v + \lambda_b = 2a + v - 1 = 2t_a$. □

Now, for the monomials $x^{\gamma_v(2a-1+u)}$, $x^{m_a^u(2^{J_a^u}\lambda_a - u + v)}$, $x^{\gamma_v(2t_a - n + 2u)}$, $x^{2^{l_a+1}\lambda_a + u}$, x^v and x^n.

Lemma 2 *Let a and b be as before, then*

1) $\gamma_v(2a-1+u) = 2t_b$ *iff* $\lambda_b - u + v = 2t_a$.

2) $2(2^{J_a^u}\lambda_a - u + v) = 2t_b$ *iff* $2t_b > n - u$ *and* $\gamma_v(2t_b - n + 2u) = 2t_a$.

3) $2a - 1 + u = v$ *iff* $2^{l_a+1}\lambda_a + u = n$ *iff* $2t_a = n - u$.

4) $2a - 1 + u > v$ *iff* $2t_a > n - u$.

5) $2(2^{J_a^u}\lambda_a - u + v) = n$ *iff* $2^{J_a^u}\lambda_a + n - u = n$.

6) $2^{l_a+1}\lambda_a + u > n$ *iff* $2t_a > n - u$ *and* $2^{l_a+1}\lambda_a + u = 2t_a + u$

Proof: $\gamma_v(2a - 1 + u) = 2t_b \Leftrightarrow 2a - 1 + u = \lambda_b \Leftrightarrow \lambda_b - u + v = 2t_a$, and thus *1)* holds. If $2(2^{J_a^u}\lambda_a - u + v) = 2t_b$, then $2t_b - n + u = 2^{J_a^u+1}\lambda_a - u > 0$ and $2t_b - n + 2u = 2^{J_a^u+1}\lambda_a \leq 2t_a$, therefore $2t_b > n - u$ and $\gamma_v(2t_b - n + 2u) = 2t_a$. Conversely, if $\gamma_v(2t_b - n + 2u) = 2t_a$, then there must exist a unique integer s, with $0 \leq s \leq l_a$, such that $2t_b - n + 2u = 2^{l_a+1-s}\lambda_a$, which implies that $2^{l_a-s}\lambda_a - u = t_b - v < 0$, and hence $l_a - s \leq J_a^u$. Suppose that $l_a - s < J_a^u$. Then $2^{l_a+1-s}\lambda_a - u = 2t_b - n + u \leq 0$, but $2t_b > n - u$, which is a contradiction. Thus, $J_a^u = l_a - s$ and *2)* holds. The remaining statements are direct. □

For monomials $x^{2^{j+1}\lambda_a - u + n}$ and $x^{\gamma_v(2t_a - n + u)}$, it is important to note that $2^{j+1}\lambda_a - u + n \leq n$ for all $1 \leq a \leq t$ and $0 \leq j < J_a^u$. Now, $2^{j+1}\lambda_a - u + n = n$ iff $j + 1 = J_a^u$ and $2(2^{J_a^u}\lambda_a - u + v) = n$. Therefore case $2^{j+1}\lambda_a - u + n = n$ is already considered by part *5)* of the previous lemma. The remaining case is considered as follows.

Lemma 3 *Let* $S_1^u = \{(a, j) \in \mathbb{Z}^2 \mid 1 \leq a \leq t,\ 0 \leq j < J_a^u$ *and* $2^{j+1}\lambda_a < u\}$ *and* $S_2^u = \{b \in \mathbb{Z} \mid 1 \leq b \leq t$ *and* $2t_b > n - u\}$*, then for each* $(a, j) \in S_1^u$ *(respect.* $b \in S_2^u$*) there exists a unique* $b \in S_2^u$ *(respect.* $(a, j) \in S_1^u$*) such that*

$$2^{j+1}\lambda_a - u + n = 2t_b \quad \text{and} \quad \gamma_v(2t_b - n + u) = 2t_a\ . \tag{11}$$

Proof: Let $b = 2^j\lambda_a - (u/2) + t + 1$. Since $0 < 2^j\lambda_a < (u/2)$, then $1 \leq t + 1 - (u/2) < b \leq t$, but $t + 1 - (u/2) < b \Leftrightarrow 2t_b > n - u$. Now, for such b, we have $2t_b - n + u = 2^{j+1}\lambda_a \leq 2^{l_a+1}\lambda_a = 2t_a$, which implies (11). Clearly, b is unique. Conversely, let $a = \gamma_v(2t_b - n + u)/2 - t$. Since $0 < 2t_b - n + u < n$, then $2t + 2 = v + 1 \leq \gamma_v(2t_b - n + u) \leq n - 2 = 4t$, which implies $1 \leq a \leq t$. Thus, for such a we have $\gamma_v(2t_b - n + u) = 2t_a$, and hence, there must exist a unique integer s, with $0 \leq s \leq l_a$, such that $2t_b - n + u = 2^{l_a+1-s}\lambda_a$. Let $j = l_a - s$, thus $2^{j+1}\lambda_a - u + n = 2t_b$, $2^{j+1} - u = 2t_b - n < 0$ and therefore $0 \leq j < J_a^u$. Finally, we must show the unicity of a and j. Suppose that the integers a' and j', with $1 \leq a' \leq t$ and $0 \leq j' < J_a^u$, are such that $2^{j'+1}\lambda_{a'} - u + n = 2t_b$. This implies that $2^{j'+1}\lambda_{a'} = 2^{j+1}\lambda_a$. Without loss of generality, suppose that $j \geq j'$ and then $\lambda_{a'} = 2^{j-j'}\lambda_a$, but since $\lambda_{a'}$ and λ_a are odd numbers, so $j - j' = 0$, $\lambda_{a'} = \lambda_a$ and $a' = a$. □

Let us note how the previous Lemma establishes a bijection between S_1^u and S_2^u, and therefore $\#S_1^u = \#S_2^u = \#\{b \in \mathbb{Z} \mid t + 1 - (u/2) < b \leq$

$t\} = (u/2) - 1$. For example, if $v = 21$ and $u = 12$, then $t = 10$, $S_1^u = \{(6,0),(6,1),(2,0),(6,2),(10,0)\}$ and $S_2^u = \{6,7,8,9,10\}$.

The analysis of monomials $x^{\gamma_v(2^{j+1}\lambda_a+u)}$ and $x^{\gamma_v(2^{j+1}\lambda_a-u)}$ is done by considering the restriction $2^{j+1}\lambda_a + u < n$, with $0 \leq j \leq l_a$.

Lemma 4 *Let* $\chi^u = \{(a,j) \in \mathbb{Z}^2 \mid 1 \leq a \leq t,\ 0 \leq j \leq l_a$ *and* $2^{j+1}\lambda_a + u < n\}$ *and* $\chi^{-u} = \{(b,k) \in \mathbb{Z}^2 \mid 1 \leq b \leq t$ *and* $J_b^u \leq k \leq l_b\}$*, then for each* $(a,j) \in \chi^u$ *(respect.* $(b,k) \in \chi^{-u}$*) there exists a unique* $(b,k) \in \chi^{-u}$ *(respect.* $(a,j) \in \chi^u$*) such that* $2^{j+1}\lambda_a + u = 2^{k+1}\lambda_b$*, and additionally*

$$\gamma_v(2^{j+1}\lambda_a + u) = 2t_b \ \ \textit{and} \ \ \gamma_v(2^{k+1}\lambda_b - u) = 2t_a. \tag{12}$$

Proof: Let $l_1 = l(u/2)$ and $l_2 = l(\lambda_a + \lambda(u/2))$. Since $0 < 2^{j+1}\lambda_a + u < n$, then there must exist a unique integer s, with $s \geq 0$, such that $v < 2^{j+1+s}\lambda_a + 2^s u < n$. Let $b = 2^{j+s}\lambda_a + 2^{s-1}u - t$ and

$$k = \begin{cases} j & \text{if } j < l_1 \\ l_1 + l_2 & \text{if } j = l_1 \\ l_1 & \text{if } j > l_1 \end{cases}.$$

For such b we have $2t + 1 = v < 2(t+b) = 2^{j+1+s}\lambda_a + 2^s u < 2v = 4t + 2$, and therefore $1 \leq b \leq t$ and $\lambda_b = \lambda(2^j\lambda_a + u/2)$. If $j < l_1$, then $k = j$ and $\lambda_b = \lambda_a + 2^{l_1-j}\lambda(u/2) \Rightarrow 2^{k+1}\lambda_b = 2^{j+1}\lambda_a + u$. If $j = l_1$, then $k = l_1 + l_2$ and $\lambda_b = \lambda(\lambda_a + \lambda(u/2)) \Rightarrow 2^{k+1}\lambda_b = 2^{l_1+1}(\lambda_a + \lambda(u/2)) = 2^{j+1}\lambda_a + u$. In a similar way, we can see that if $j > l_1$, then $2^{k+1}\lambda_b = 2^{j+1}\lambda_a + u$. Thus $2^{j+1}\lambda_a + u = 2^{k+1}\lambda_b$ in any case, and hence, $\gamma_v(2^{j+1}\lambda_a + u) = \gamma_v(2^{k+1}\lambda_b) = 2t_b$. The right hand side of (12) is obtained in an analogous way. On the other hand, since $u < 2^{k+1}\lambda_b = 2^{j+1}\lambda_a + u \leq 2t_b = 2^{l_b+1}\lambda_b$, we deduce that $J_b^u \leq k \leq l_b$ (by definition of l_b and J_b^u). Now, suppose that $(b',k') \in \chi^{-u}$ is such that $2^{j+1}\lambda_a + u = 2^{k'+1}\lambda_{b'}$. This implies that $2^{k'+1}\lambda_{b'} = 2^{k+1}\lambda_b$ and therefore $b' = b$ and $k' = k$.

Conversely, let $l_3 = l(\lambda_a - \lambda(u/2))$. Since $0 < 2^{k+1}\lambda_b - u < n$, then there must exist a unique integer s, with $s \geq 0$, such that $v < 2^{k+1+s}\lambda_b - 2^s u < n$. Let $a = 2^{k+s}\lambda_b - 2^{s-1}u - t$ and

$$j = \begin{cases} k & \text{if } k < l_1 \\ l_1 + l_3 & \text{if } k = l_1 \\ l_1 & \text{if } k > l_1 \end{cases}.$$

For such a we have $2t+1 = v < 2(t+a) = 2^{k+1+s}\lambda_b - 2^s u < 2v = 4t+2$, and therefore $1 \leq a \leq t$ and $\lambda_a = \lambda(2^k\lambda_a - u/2)$. By taking into consideration the first part of this proof, the remaining part is routine. □

In an analogous way as with Lemma 3, the previous one establishes a bijection between χ^u and χ^{-u} and therefore $\#\chi^u = \#\chi^{-u}$. For example, if $v = 11$ and $u = 6$, then $t = 5$, $\chi^u = \{(1,0),(1,1),(2,0),(3,0),(3,1),(3,2),(5,0)\}$ and $\chi^{-u} = \{(1,1),(4,0),(5,1),(3,2),(5,0),(2,0),(3,3)\}$.

There are two remaining cases for the monomial $x^{\gamma_v(2^{j+1}\lambda_a+u)}$: $2^{j+1}\lambda_a + u = n$ and $2^{j+1}\lambda_a + u > n$. Note that both cases imply that $j = l_a$ (since $v < n - u \leq 2^{j+1}\lambda_a < n \Rightarrow 2^{j+1}\lambda_a = 2t_a$ and $j = l_a$), and therefore both cases are already covered by *3)* and *6)*, in Lemma 2.

As we can see from (10), the monomials in $\tilde{R}_{v+t_a}(x)$ can be classified into three categories: those whose degree is equal to v, those whose degree is an even number greater than or equal to n, and those whose degree is an even number greater than v and less than n. Parts *3)*, *4)*, *5)* and *6)* in Lemma 2, show that for any monomial in the first two categories, there exists another monomial in the same row polynomial $\tilde{R}_{v+t_a}(x)$ which annihilates it. For this reason, we must never expect to find such kind of monomials in the reduction of $\tilde{R}_{v+t_a}(x)$. On the other hand, and for the third category, parts *1)* and *2)* in Lemma 2, and the remaining lemmas in this section, show that for any pair of integers a and b, with $1 \leq a, b \leq t$, the monomial x^{2t_b} is in the row polynomial $\tilde{R}_{v+t_a}(x)$ iff the monomial x^{2t_a} is in $\tilde{R}_{v+t_b}(x)$. Thus, we have proved the following result.

Theorem 1 *The $t \times t$ submatrix $\mathcal{B}$ is symmetric.*

Besides the symmetric shape of $\mathcal{B}$, there are two more properties, which will be important in order to prove the reducibility of self-reciprocal binary pentanomials of Type 2.

4 Two Relevant Properties of these Symmetric Submatrices

For a given row (or column) in $\mathcal{B}$, we are interested in its diagonal element, and in the parity of the number of ones in such a row. The next result shows a relationship between this parity and this diagonal element.

Theorem 2 *The diagonal element, in any row of $\mathcal{B}$, is equal to one iff the number of ones in the row has odd parity.*

Proof: Since submatrix $\mathcal{B}$ is symmetric, the value of the diagonal element in its a-th row, with $a = 1, 2, \ldots, t$, will be determined by the number of times the monomial x^{2t_a} appears in (10). A direct inspection of (10), shows that this monomial is considered in lines 1, 2 and 5 of this equation. Looking at the first line, we can see that monomial x^{2t_a}, and another four monomials, are considered just one time. The second line tells us that x^{2t_a} is considered J_a^u times, and in every instance another two monomials are also considered. The fifth line (together with the fourth) shows that monomial x^{2t_a}, and another four monomials, will be considered iff $2t_a > n - u$. Thus, and since the number of monomials in line 3 is an even number, it follows that the monomial x^{2t_a} appears in (10) an odd number of times, iff the total number of monomials for this equation is also an odd number. □

We are now interested in the number of zeros in the diagonal of the submatrix $\mathcal{B}$. In order to present a result in this direction, we first need a preliminary result.

Notation: Let u and t be as before and let s be a positive integer ($s \geq 0$). For each value of s, t and u, we will denote by $\Omega_{s,t}^u$ the set of integers given by

$$\Omega_{s,t}^u = \{a \in \mathbb{Z} \mid 1 \leq a \leq t \text{ and } J_a^u = s\} .$$

Note that $\sum_s \#\Omega_{s,t}^u = t$. For example, if $u = 10$ and $t = 8$, then $\Omega_{0,8}^{10} = \{1, 3, 5, 6, 7\}$, $\Omega_{1,8}^{10} = \{2, 4\}$, $\Omega_{2,8}^{10} = \phi$, $\Omega_{3,8}^{10} = \{8\}$ and $\Omega_{s,t}^u = \phi$, for all $s \geq 4$.

Lemma 5 *With the previous notation, we have*

$$(\sum_{s \text{ odd}} \#\Omega_{s,t}^u) \bmod 2 = \begin{cases} 0 & \text{if } u/2 \text{ is an even number} \\ 1 & \text{otherwise} \end{cases} .$$

Proof: Suppose that u is such that $2 \leq u < 2t = v-1$. Let $b = \gamma_v(u+2)/2 - t$. Since $v + 1 \leq \gamma_v(u + 2) \leq 4t$, it follows that $1 \leq b \leq t$. Now, since $2^{J_a^u+1}\lambda_a \geq u + 2$ for all $a = 1, 2, ..., t$, and since $2^{J_b^u}\lambda_b \leq u$ and $\lambda_b = \lambda(u + 2)$, then $2^{J_a^u+1}\lambda_a = u + 2$ iff $a = b$. In other words, we have $J_a^{u+2} = J_a^u + \delta(a = b)$, for all $a = 1, 2, ..., t$. Thus, $b \in \Omega_{J_b^u,t}^u$ and $b \in \Omega_{J_b^u+1,t}^{u+2}$. Hence

$$\begin{aligned} \#\Omega_{J_b^u,t}^{u+2} &= \#\Omega_{J_b^u,t}^u - 1 , \\ \#\Omega_{J_b^u+1,t}^{u+2} &= \#\Omega_{J_b^u+1,t}^u + 1 , \\ \#\Omega_{s,t}^{u+2} &= \#\Omega_{s,t}^u \text{ for any integer } s \geq 0, \text{ with } s \neq J_b^u \text{ and } s \neq J_b^u + 1 . \end{aligned}$$

Since $\sum_{s \text{ odd}} \#\Omega_{s,t}^2 = 1$, then a recursive application of the previous set of equations gives us the desired result. □

Theorem 3 *The number of zeros in the diagonal of the submatrix $\mathcal{B}$ has odd parity.*

Proof: It is deduced from the proof of Theorem 2, that the diagonal element in the a-th row of the submatrix $\mathcal{B}$, will be zero iff any of the next two conditions are satisfied: J_a^u is odd and $\delta(2t_a > n-u) = 0$ or J_a^u is an even number and $\delta(2t_a > n-u) = 1$. But note that J_a^u, in the a-th row of $\mathcal{B}$, is odd iff $a \in \cup_{s\ odd}\Omega_{s,t}^u$. Thus the claimed result follows from the previous lemma and the fact that the number of rows in $\mathcal{B}$ that satisfy $2t_a > n-u$, is $(u/2)-1$. □

Taking into consideration these new properties of $\mathcal{B}$, we introduce the following definition.

Definition 1 *A square symmetric binary matrix, is said to be a Matrix of Type 2, if such a matrix satisfies the following two conditions:*

1) *The diagonal element, in any row of the matrix, is equal to one iff the number of ones in the row has odd parity.*

2) *The number of zeros on its diagonal has odd parity.*

5 The Result

The main goal of this section is to show that all self-reciprocal binary pentanomials of Type 2 have an even number of irreducible polynomial factors. To get to this result, we first have to show that the nullity of any matrix of Type 2 has odd parity.

Lemma 6 *Let A be a non-null square symmetric binary matrix of size $t \times t$, whose diagonal entries are all equal to zero. If such a matrix also satisfies condition 1) in Definition 1, then there exist an equivalent symmetric binary matrix which satisfies the same condition, and which has a nonzero diagonal with an even number of ones on it.*

Proof: For $i, j = 1, 2, \ldots, t$, we will denote by $a_{i,j}$, R_i and C_i the respective entries, rows and columns of A. The equivalent matrix that we are searching for, will be obtained in two steps. In each step we construct a matrix equivalent to A. We will denote by $A^{(1)}$, $a_{i,j}^{(1)}$, $R_i^{(1)}$ and $C_i^{(1)}$ the first matrix and its corresponding components, whereas for the second one, we will use the notation

$A^{(2)}$, $a^{(2)}_{i,j}$, $R^{(2)}_i$ and $C^{(2)}_i$. By hypothesis there exist integers r and s, with $1 \leq r, s \leq t$, such that $r \neq s$ and $a_{r,s} = 1$. For such r let $\mathcal{J}_r = \{j \,|\, 1 \leq j \leq t \text{ and } a_{r,j} = 1\}$. Note how $\#\mathcal{J}_r = w_h(R_r) = \textit{even number greater than } 0$, where $w_h(\cdot)$ stands for the *Hamming weight function* (see for example [3]). In order to obtain $A^{(1)}$, we add the r-th row of A to its s-th row, that is, we perform: $R^{(1)}_i = R_i + \delta(i = s)R_r$. If we denote by $\hat{e}_s$ the s-th canonical column vector of length t (*ie*, the column vector of length t with all zeros except for the s-th entry, which contains a 1), then $C^{(1)}_j = C_j + a_{r,j}\hat{e}_s$, for all $j = 1, 2, \ldots, t$. Since $C^{(1)}_r = C_r$, then the matrix $A^{(2)}$ is constructed by doing: $C^{(2)}_j = C^{(1)}_j + a_{r,j}\delta(j \neq s)C_r$, or equivalently, $C^{(2)}_j = C_j + a_{r,j}\hat{e}_s + a_{r,j}\delta(j \neq s)C_r = C_j + \delta(j = s)\hat{e}_s + a_{r,j}\delta(j \neq s)(C_r + \hat{e}_s)$, for all $j = 1, 2, \ldots, t$. Therefore

$$a^{(2)}_{i,j} = a_{i,j} + \delta(i = j = s) + a_{r,j}\delta(j \neq s)\delta(i \neq s)a_{i,r} \; .$$

From the previous equation, and since A is symmetric, we can see that $A^{(2)}$ is also a symmetric matrix. Since $w_h(C_r + \hat{e}_s) = \textit{odd number}$, and $w_h(C_j) = \textit{even number}$, then we have $w_h(C^{(2)}_j) = \textit{odd number}$ iff $j \in \mathcal{J}_r$ iff $a^{(2)}_{j,j} = 1$. □

Theorem 4 *Let A be a $t \times t$ symmetric binary matrix of Type 2, then the nullity of such a matrix is an odd number.*

Proof: If A is the null matrix, then t is an odd number and the claim follows. Now, if A is not the null matrix but has a zero diagonal, then t is again an odd number and by using Lemma 6, we can find an equivalent symmetric binary matrix of Type 2 with a non zero diagonal. Thus, without loss of generality we can suppose that A has a non zero diagonal. If $a_{i,j}$ and R_i, for $i, j = 1, 2, \ldots, t$, denote the entries and the rows of matrix A, then there must exist an integer s, with $1 \leq s \leq t$, such that $a_{s,s} = 1$. Applying row operations on matrix A we construct a row equivalent matrix $\tilde{A}$, in such a way that the s-th column of $\tilde{A}$ will correspond to the s-th canonical column vector $\hat{e}_s$, of length t. That is, if $\tilde{a}_{i,j}$ and $\tilde{R}_i$, with $i, j = 1, 2, \ldots, t$, denote the entries and the rows of $\tilde{A}$, then such rows are given by $\tilde{R}_i = R_i + a_{i,s}\delta(i \neq s)R_s$. Or in an equivalent way

$$\tilde{a}_{i,j} = a_{i,j} + a_{i,s}\delta(i \neq s)a_{s,j} \; .$$

Since A is symmetric, then $\tilde{a}_{i,j} = \tilde{a}_{j,i}$, for all $i, j = 1, 2, \ldots, t$, with $i, j \neq s$. This means that the $t-1 \times t-1$ submatrix $\mathcal{A}$, obtained from $\tilde{A}$ by deleting its s-th row and its s-th column, is symmetric. We claim that $\mathcal{A}$ is a matrix of Type 2. In order to see that, we observe that $w_h(R_s) = \textit{odd number}$ and $\tilde{a}_{i,i} = a_{i,i} + 1 \Leftrightarrow a_{i,s} = 1$ for all $i \neq s$. Thus, $\#\{i \,|\, i = 1, 2, \ldots, t,\ i \neq s,\ \text{and } \tilde{a}_{i,i} \neq a_{i,i}\} = \textit{even number}$, and hence submatrix $\mathcal{A}$ has an odd number of zeros on its diagonal (since A also has the same kind of diagonal). Similar arguments prove that $\mathcal{A}$ satisfies also condition *1)* in Definition 1. Clearly, the nullity of A is equal to the nullity of $\mathcal{A}$. If $\mathcal{A}$ is the null matrix, then we have the claim. If is not, we re-apply the previous procedure to matrix $\mathcal{A}$. Thus, a recursive application of this procedure give us the desired result. □

We are now able to prove the result.

Theorem 5 *If $P(x)$ is a self-reciprocal binary pentanomial of Type 2, then it has an even number of irreducible polynomial factors.*

Proof: Using $P(x)$ in (1), we obtain a square binary matrix B, such that $Nullity(B) = \textit{number of irreducible polynomial factors of } P(x)$. Through the construction seen in Section 1, we can find a square binary matrix $\mathcal{B}$, such that $Nullity(B) = Nullity(\mathcal{B}) + 1$. By means of Theorems 1, 2 and 3, we prove that $\mathcal{B}$ is a matrix of Type 2. Finally, Theorem 4 show us that $Nullity(\mathcal{B}) = \textit{odd number}$. □

6 Conclusions and Final Remarks

As we have seen, we proved, through a very specific construction, the reducibility of all self-reciprocal binary pentanomial of Type 2. Via this construction, we associated a binary symmetric singular submatrix to each self-reciprocal binary pentanomial of Type 2. Nevertheless, it is not clear to the author, if a similar construction, for self-reciprocal binary pentanomial of Type 3 or 4, is possible. That is, we do not know if it a construction is possible, by means of which, we can also associate a binary symmetric matrix (although not necessarily singular) to each self-reciprocal binary pentanomial of Type 3 or 4. Besides, in this case, we cannot directly use the Berlekamp Algorithm, since some of these pentanomials could have repeated factors. More precisely, if $P(x) = x^{2v} + x^{2v-u} + x^v + x^u + 1$ is a pentanomial of Type 3 or 4 (u is odd, and v is even or odd), then it can be proved that, if v is even, then such pentanomial has repeated factors iff $v-u$ is a multiple of three and $3((v-u)/3, v)$

$\not| \, v$. If v is odd, then $P(x)$ has repeated factors iff v is a multiple of three and $3(v/3, v-u) \not| \, (v-u)$. Considering factor repetition, and with the help of computer programs, we analyzed pentanomials of these types and we conjecture that all self-reciprocal binary pentanomial of Type 3 or 4 have an odd number of irreducible polynomial factors (and for this reason, some of them are irreducible). For example: $P(x) = 1 + x^9 + x^{15} + x^{21} + x^{30}$ is an irreducible self-reciprocal binary pentanomial of Type 4. Note also that this pentanomial disproves the conjecture settled in [4].

Acknowledgments

The author wishes to thank Luis Cota for helpful numerical computations.

References

[1] Kenneth H. Hicks, Gary L. Mullen and Ikuro Sato, *Distribution of Irreducible Polynomial over F_2*, Proceedings of the Sixth International Conference on Finite Fields and Applications (Fq6), held at Oaxaca, Mexico, (2001), 177-186.

[2] R. Lidl, H. Niederreitter, *Introduction to Finite Fields and Their Applications*, Revised Edition, Cambridge University Press, Cambridge, 1994.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, (1977).

[4] Joseph L. Yucas and Gary L. Mullen, *Self-Reciprocal Irreducible Polynomials Over Finite Fields*, Designs, Codes and Cryptography, **33** (2004), 275-281.

Received: October 14, 2006