International Journal of Algebra, Vol. 9, 2015, no. 3, 131 - 145
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2015.5210

Self-Invertible Cubic (Quartic) Permutation Polynomials over $\mathbb{Z}_{p^n}$ with $p > 7$ ($p > 17$) a Prime and Gröbner Bases

Javier Diaz-Vargas

Universidad Autónoma de Yucatán, Facultad de Matemáticas
Periférico Norte Tablaje 13615, 97119, Mérida, Yucatán

Carlos Jacob Rubio-Barrios

Universidad Autónoma de Yucatán, Facultad de Matemáticas
Periférico Norte Tablaje 13615, 97119, Mérida, Yucatán

Horacio Tapia-Recillas

Universidad Autónoma Metropolitana-I, Departamento de Matemáticas
09340, Distrito Federal, México

Abstract

Necessary and sufficient conditions for cubic (quartic) permutation polynomials to be self-invertible over the ring $\mathbb{Z}_{p^n}$ where $p > 7$ ($p > 17$) is a prime number are given, and completely determined. The characterization of these permutations are given by relations on the coefficients of the polynomial which resulted in a Gröbner basis with respect to some lexicographic order of certain ideals.

Mathematics Subject Classification: 11T06, 13M10

Keywords: Permutation polynomials, Gröbner basis

1 Introduction

The Symmetric group S_n, i.e., the group of permutations on n symbols has been one of the most interesting groups and its applications cover several areas in both "pure" and "applied" Mathematics. With the advance of information technology the symmetric group is of great importance: for example, in the design of symmetric cipher systems such as the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES), the Substitution boxes (S-boxes) are permutations; in error detecting-correcting linear (block) codes permutations are used to describe equivalent codes. A main component in the design of turbo codes is a pair of convolutional codes and an interleaver between them, which is just a permutation. Since the inverse of an interleaver is used in the decoding process, easy and computationally low cost methods are required to generate permutations, so it would be interesting to determine self-invertible permutations. One way to determine permutations is by means of polynomials which have been extensively studied over finite fields ([4]). For practical purposes in turbo coding, permutations on sets with cardinality 2^n, (e.g. $n = 7, 8, 9, 10$) are fundamental. In [8] results on interleavers based on permutation polynomials are presented and in [9] results on self-invertible quadratic permutation polynomials are discussed. Also, the authors undertook the study of self-invertible permutation polynomials of degree two and three over the ring $\mathbb{Z}_{p^n}$ of integers modulo p^n for various values of the prime p and the integer $n > 1$ ([3]). In this note, necessary and sufficient conditions for a cubic (quartic) polynomial over the ring $\mathbb{Z}_{p^n}, p > 7$, $(p > 17)$ to determine a self-invertible permutation are given. Furthermore, all of these permutation polynomials are determined. These necessary and sufficient conditions are given by relations on the coefficients of the polynomials and it turns out that these relations determine a (strong) Gröbner basis of certain ideals.

The manuscript is organized as follows: the main result in Section 2 is the characterization of self-invertible quartic permutation polynomials over the ring $\mathbb{Z}_{p^n}$ for $p > 13$ a prime and $n > 1$ an integer. In Section 3, using the fact that the ring $\mathbb{Z}_{p^n}$ is a finite chain ring, self-invertible cubic (quartic) permutation polynomials are determined over this ring for $p > 7$, $(p > 17)$. Finally, in Section 4, after recalling facts on (strong) Gröbner bases it is shown that relations on the coefficients for a cubic (quartic) polynomial to be self-invertible determine such bases of some ideals in the polynomial ring in three (cubic) and four (quartic) variables over $\mathbb{Z}_{p^n}$.

2 Self-Invertible Permutation Polynomials over $\mathbb{Z}_{p^n}$, p a prime

Let $R \neq 0$ be a commutative ring with unity. A polynomial $f(x) = a_1x + a_2x^2 + \cdots + a_dx^d \in R[x]$ with $a_d \neq 0$ is self-invertible if $f(f(\alpha)) = \alpha$ for all $\alpha \in R$.

The following result generalizes Theorem 3.2 of [3].

Theorem 2.1. *Let $n \geq 1$ be an integer, $f(x) = a_1x + a_2x^2 + \cdots + a_dx^d \in \mathbb{Z}_{p^n}[x]$ with $d \geq 3$, $a_d \neq 0$, and p be a prime such that $p > d^2 - 1$. Then, $f(x)$ is self-invertible if and only if the coefficients of $g(x) = f(f(x)) - x$ are all equal to 0.*

Proof. Suppose that $f(x)$ is self-invertible. Then, $g(a) = 0$ for all $a \in \mathbb{Z}_{p^n}$. In particular, $g(u) = 0$ for all $u = 1, 2, \ldots, d^2$, each one a unit in $\mathbb{Z}_{p^n}$ since $p > d^2 - 1$. Then,

$$g(u) \cdot u^{-1} = 0 \text{ for all } u = 1, 2, \ldots, d^2. \tag{1}$$

Let $V(x_1, x_2, \ldots, x_{d^2})$ be the $d^2 \times d^2$ Vandermonde matrix in the indeterminates $x_1, x_2, \ldots, x_{d^2}$ and let $\Delta = V(1, 2, \ldots, d^2)$ where $1, 2, \ldots, d^2 \in \mathbb{Z}_{p^n}$. For an integer $m \in \{1, 2, \ldots, d^2\}$ let $m! = m(m-1)\cdots 2 \cdot 1$ (the product taken in the ring $\mathbb{Z}_{p^n}$). It is easy to see that the determinant of Δ is

$$\prod_{1 \leq i < j \leq d^2} (j - i) = \prod_{i=1}^{d^2-1} k!,$$

which is a unit in the ring $\mathbb{Z}_{p^n}$, and therefore Δ is invertible. Let $\alpha = (\alpha_1, \ldots, \alpha_{d^2})$, where $\alpha_1, \ldots, \alpha_{d^2}$ are the coefficients of $g(x)$. From relation (1) the linear system

$$\Delta \alpha^t = 0,$$

has only the trivial solution since the matrix Δ is invertible, proving the claim. The converse is clear. □

If $f(x) = ax + bx^2 + cx^3 + dx^4 \in R[x]$ is a quartic permutation polynomial, it is

easily seen that the coefficients of $g(x) = f(f(x)) - x$ are:

$$\alpha_1 = a^2 - 1, \tag{2}$$
$$\alpha_2 = ab(1 + a), \tag{3}$$
$$\alpha_3 = a(a^2c + 2b^2 + c), \tag{4}$$
$$\alpha_4 = ad + 3ca^2b + 2abc + b^3 + a^4d, \tag{5}$$
$$\alpha_5 = 4da^3b + 3a^2c^2 + 2bad + 3cab^2 + 2b^2c, \tag{6}$$
$$\alpha_6 = 6abc^2 + cb^3 + 3ca^2d + bc^2 + 6da^2b^2 + 2b^2d + 4da^3c, \tag{7}$$
$$\alpha_7 = 4a^3d^2 + 2bcd + 4dab^3 + 12da^2bc + 3b^2c^2 + 6cabd + 3ac^3, \tag{8}$$
$$\alpha_8 = 6ac^2d + 3bc^3 + bd^2 + 3cb^2d + db^4 + 12dab^2c + 12a^2bd^2 + 6da^2c^2, \tag{9}$$
$$\alpha_9 = 12a^2cd^2 + c^4 + 3cad^2 + 6bc^2d + 12dabc^2 + 4db^3c + 12ab^2d^2, \tag{10}$$
$$\alpha_{10} = 24abcd^2 + 6db^2c^2 + 4dac^3 + 3c^3d + 3cbd^2 + 6a^2d^3 + 4b^3d^2, \tag{11}$$
$$\alpha_{11} = 4dbc^3 + 12ac^2d^2 + 3c^2d^2 + 12abd^3 + 12b^2cd^2, \tag{12}$$
$$\alpha_{12} = dc^4 + 6b^2d^3 + cd^3 + 12bc^2d^2 + 12acd^3, \tag{13}$$
$$\alpha_{13} = 4c^3d^2 + 12bcd^3 + 4ad^4, \tag{14}$$
$$\alpha_{14} = 4bd^4 + 6c^2d^3, \tag{15}$$
$$\alpha_{15} = 4cd^4, \tag{16}$$
$$\alpha_{16} = d^5. \tag{17}$$

Theorem 2.2. *Let R be a commutative ring with unity, $f(x) = ax + bx^2 + cx^3 + dx^4$ a quartic polynomial over R and assume that 2, 3 and 5 are units in R. Then, relations* (2) *to* (17) *are all zero if and only if*

$$a^2 - 1 = b(1 + a) = b^2 + c = 2b^4 - 3bd = 4d^2 + 3b^3d = 17bd^2 = b^2d^2 = d^3 = 0.$$

Proof. Suppose that relations *(2)* to *(17)* are all zero. Relation *(2)* states that $a^2 = 1$ and hence a is a unit. Thus, from relations *(3)* and *(4)* it follows that $b = -ab$ and $c = -b^2$. Substituting these new relations in a^2, b and c, in relations *(5)* to *(17)* the following set of relations are obtained:

$$
\begin{aligned}
0 &= d(1+a)\\
0 &= 4b^4 - 6bd\\
0 &= 6b^5 - 9b^2d = 2^{-1}\cdot 3b(4b^4 - 6bd)\\
0 &= 6b^6 - 12b^3d - 4d^2 = 2^{-1}\cdot 3b^2(4b^4 - 6bd) - 4d^2 - 3b^3d\\
0 &= -3b^7 + 10b^4d + 13bd^2 = -2^{-2}(3b^3 - 2^{-1}\cdot 11d)(4b^4 - 6bd) + 2^{-2}\cdot 85bd^2\\
0 &= b^8 - 10b^5d - 21b^2d^2 = 2^{-3}(2b^4 - 17bd)(4b^4 - 6bd) - 2^{-2}\cdot 135b^2d^2\\
0 &= 7b^6d + 25b^3d^2 + 6d^3 = 2^{-2}\cdot 7b^2d(4b^4 - 6bd) + 2^{-1}\cdot d^2(71b^3 + 12d)\\
0 &= -4b^7d - 21b^4d^2 - 12bd^3 = -2^{-2}(4b^3d + 27d^2)(4b^4 - 6bd) - 2^{-1}\cdot 105bd^3\\
0 &= b^8d + 12b^5d^2 + 17b^2d^3 = 2^{-3}(2b^4d + 27bd^2)(4b^4 - 6bd) + 2^{-2}\cdot 149b^2d^3\\
0 &= -4b^6d^2 - 12b^3d^3 - 4d^4 = -b^2d^2(4b^4 - 6bd) - 18b^3d^3 - 4d^4\\
0 &= 6b^4d^3 + 4bd^4 = 2^{-1}\cdot 3d^3(4b^4 - 6bd) + 13bd^4\\
0 &= -4b^2d^4\\
0 &= d^5
\end{aligned}
$$

From relation (4) of this set of relations, $4d^2 + 3b^3d = 0$. Multiplying this last relation by d and since $b^2d^2 = 0$ from relation (6), it follows that $4d^3 = 0$ and since 2 is a unit in the ring, $d^3 = 0$. The converse is straightforward. □

The following result gives a characterization for a quartic permutation polynomial over the ring $\mathbb{Z}_{p^n}$ for primes $p > 13$ to be self-invertible .

Theorem 2.3. *Let $n \geq 1$ be an integer, $p > 13$ a prime and $f(x) = ax + bx^2 + cx^3 + dx^4$ a quartic permutation polynomial over $\mathbb{Z}_{p^n}$. Then, $f(x)$ is self-invertible if and only if*

$$a + 1 = b^2 + c = 2b^4 - 3bd = 4d^2 + 3b^3d = 17bd^2 = b^2d^2 = d^3 = 0.$$

Proof. If $f(x)$ is self-invertible, Theorem 2.1 implies that the coefficients α_i, $i = 1, \ldots, 16$, of $g(x)$ are all equal to zero (since $p > 4^2 - 1$), and by Theorem 2.2,

$$a^2 - 1 = b(1 + a) = b^2 + c = 2b^4 - 3bd = 4d^2 + 3b^3d = 17bd^2 = b^2d^2 = d^3 = 0.$$

Since $\mathbb{Z}_{p^n}$ is a local ring, it does not have nontrivial idempotents (distinct from 0 and 1), and since the characteristic of $\mathbb{Z}_{p^n}$ is not a power of 2, the condition $a^2 = 1$ implies that the idempotents are of the form $2^{-1}(1 + a)$ (see Theorem VII.7 and Exercise VII.12 of [5]). Therefore, $a = -1$ or $a = 1$. If $a = 1$ then $b(1 + a) = 2b = 0$ and hence $b = 0$. Thus, from relation (5) we have $\alpha_4 = 2d = 0$ and then $d = 0$ which is a contradiction since the degree of $f(x)$ is 4. Then $a = -1$ or $a + 1 = 0$.

Conversely, if relation on the statement of the Theorem hold, then $a^2 - 1 = b(1 + a) = b^2 + c = 2b^4 - 3bd = 4d^2 + 3b^3d = 17bd^2 = b^2d^2 = d^3 = 0$, and from Theorem 2.2 it follows that all coefficients of $f(f(x)) - x$ are zero. Finally, Theorem 2.1 implies that $f(x)$ is self-invertible. □

Remark 2.4. *In Corollary 3.4 of [3] it was shown that for primes $p > 7$, a cubic permutation polynomial $f(x) = ax + bx^2 + cx^3 \in \mathbb{Z}_{p^n}[x]$ is self-invertible if and only if*

$$a^2 - 1 = b(1 + a) = b^2 + c = c^2 = 0.$$

However, as in Theorem 2.3, the condition $a^2 - 1 = 0$ is also equivalent to the condition $a + 1 = 0$. Indeed, since $\mathbb{Z}_{p^n}$ is a local ring whose characteristic is not a power of 2 and a is an involution, it follows that $a = 1$ or $a = -1$ (Theorem VII.7 and Exercise VII.12 of [5]). If $a = 1$, then $b(1 + a) = 2b = 0$ which implies that $b = 0$ and from $b^2 + c = 0$ we obtain $c = 0$ which is a contradiction. Thus, $a = -1$. Conversely, if $a + 1 = 0$ it follows immediately that $a^2 - 1 = (a + 1)(a - 1) = 0$.

Therefore, $f(x)$ is self-invertible if and only if $a + 1 = b^2 + c = c^2 = 0$.

3 Description of Cubic (Quartic) Self-invertible Permutation Polynomials over $\mathbb{Z}_{p^n}$ for primes $p > 7$ $(p > 17)$,

Before giving a description of cubic and quartic self-invertible permutation polynomials over $\mathbb{Z}_{p^n}$ for some primes p, recall that a *chain ring* is a ring whose ideals are linearly ordered by inclusion. A chain ring with finitely many ideals is called a *finite-chain ring*. For example, the ring $\mathbb{Z}_{p^n}$ is a finite-chain ring for any prime p and any positive integer n, since any ideal is of the form $\langle p^i \rangle$ for $i = 0, 1, \ldots, n$, and the lattice of these ideals is such that

$$\mathbb{Z}_{p^n} = \langle 1 \rangle \supset \langle p \rangle \supset \cdots \supset \langle p^{n-1} \rangle \supset \langle p^n \rangle = 0.$$

The following well-known properties of a finite-chain ring ([6]) will be needed later.

Theorem 3.1. *Let A be a finite-chain ring. Then*

1. *A is a principal ideal ring.*
2. *A is a local ring with maximal ideal M.*
3. *The elements of M are nilpotent and the elements of $A \setminus M$ are units.*
4. *If γ is a fixed generator of M and ν is the nilpotency index of γ i.e. the smallest positive integer for which $\gamma^\nu = 0$, then*
   (a) *the distinct proper ideals of A are $\langle \gamma^i \rangle_A$, $i = 1, \ldots, \nu - 1$,*
   (b) *for any element $a \in A \setminus \{0\}$ there is a unique i and a unit $u \in A$ such that $a = u\gamma^i$ where $0 \leq i \leq \nu - 1$ and u is unique modulo $\gamma^{\nu - i}$.*

The next result determines all self-invertible cubic permutation polynomials.

Theorem 3.2. *Let $n \geq 1$ be an integer and $p > 7$ be a prime. The self-invertible cubic permutation polynomials over $\mathbb{Z}_{p^n}$ are of the form*

$$f(x) = -x + up^k x^2 + vp^{2k} x^3$$

where k is an integer such that $\frac{n}{4} \leq k < \frac{n}{2}$, and u, v are units in $\mathbb{Z}_{p^n}$ such that p^{n-2k} divides $(u^2 + v)$.

Proof. Let $f(x) = ax + bx^2 + cx^3$ be a self-invertible cubic permutation polynomial over $\mathbb{Z}_{p^n}$. Since $c \neq 0$, from Theorem 3.1, $c = vp^l$ with $0 \leq l < n$ and v a unit. On the other hand, by Remark 2.4, $a = -1$ and $b^2 + c = 0$. Thus, if $b = 0$ relation $b^2 + c = 0$ implies that $c = 0$ which is a contradiction. Therefore $b \neq 0$ and from Theorem 3.1, $b = up^k$ with $0 \leq k < n$ and u a unit. Hence

$$0 = b^2 + c = u^2 p^{2k} + vp^l.$$

If $l < 2k$ then $p^l(u^2 p^{2k-l} + v) = 0$ and $u^2 p^{2k-l} + v$ is a unit. Then $p^l = 0$, therefore $c = 0$ which is a contradiction.
If $l > 2k$ then $p^{2k}(u^2 + vp^{l-2k}) = 0$ and $u^2 + vp^{l-2k}$ is a unit. Then $p^{2k} = 0$ and then $b^2 = 0$. It follows that $c = 0$ which is a contradiction.
Hence $l = 2k < n$ and $0 = p^{2k}(u^2 + v)$ implies that $p^{n-2k} \mid (u^2 + v)$. Also, from Remark 2.4, $0 = c^2 = v^2 p^{2l}$ which implies that $2l \geq n$, and therefore $k \geq \frac{n}{4}$.
Conversely, if $a = -1$, $b = up^k$ and $c = vp^{2k}$ where $\frac{n}{4} \leq k < \frac{n}{2}$ and u, v are units such that $p^{n-2k} \mid (u^2 + v)$, then it is straightforward to see that $a + 1 = b^2 + c = c^2 = 0$, and the result follows from Remark 2.4. □

Theorem 3.3. *Let $n \geq 1$ be an integer and $p > 17$ a prime. The self-invertible quartic permutation polynomials $f(x) = ax + bx^2 + cx^3 + dx^4$ over $\mathbb{Z}_{p^n}$ are as follows:*

1. *If $c = 0$, $f(x) = -x + up^k x^2 + wp^m x^4$ where $\frac{n}{2} \leq k \leq n$, $\frac{n}{2} \leq m < n$, and u, w are units.*
2. *If $c \neq 0$, $f(x) = -x + up^k x^2 + vp^{2k} x^3 + wp^m x^4$ where $k < \frac{n}{2}$, u, v and w are units such that p^{n-2k} divides $(u^2 + v)$, $m < n$, and*
   (a) *If $m < 3k$, then $f(x)$ is self-invertible if and only if $k + m \geq n$ and $m \geq \frac{n}{2}$.*
   (b) *If $m = 3k$, then $f(x)$ is self-invertible if and only if $\frac{n}{6} \leq k < \frac{n}{4}$ and $p^{n-4k} \mid (2u^2 - 3w)$, or $k \geq \frac{n}{4}$.*
   (c) *If $m > 3k$, then $f(x)$ is self-invertible if and only if $k \geq \frac{n}{4}$.*

Proof. Let $f(x) = ax + bx^2 + cx^3 + dx^4$ be a quartic permutation polynomial over $\mathbb{Z}_{p^n}$, $p > 17$. Then, $d \neq 0$ and Proposition 3.1 implies that $d = wp^m$ with $0 \leq m < n$ and w a unit.

1. $c = 0$. Suppose that $f(x)$ is self-invertible. Theorem 2.3 implies that $a = -1$, $b^2 + c = 0$ and $4d^2 + 3b^3d = 0$. Since $c = 0$, $b^2 = 0$ and so $d^2 = 0$. From $0 = d^2 = w^2p^{2m}$ it follows that $2m \geq n$ and so $\frac{n}{2} \leq m < n$. If $b = 0$, then $f(x) = -x + wp^mx^4$. If $b \neq 0$, $b = up^k$ where $0 \leq k < n$ and u a unit, by Theorem 3.1. Now, from $0 = b^2 = u^2p^{2k}$, $2k \geq n$ and therefore $\frac{n}{2} \leq k < n$.
Conversely, if $f(x) = -x + up^kx^2 + wp^mx^4$ where $\frac{n}{2} \leq k \leq n$, $\frac{n}{2} \leq m < n$, and u, w are units, it follows that $a = -1$, $b = up^k$ and $d = wp^m$. Thus $b^2 + c = b^2 = u^2p^{2k} = 0$ since $2k \geq n$; $2b^4 - 3bd = -3bd = -3uwp^{k+m} = 0$ since $k+m \geq \frac{n}{2} + \frac{n}{2} = n$; $4d^2 + 3b^3d = 4d^2 = 4w^2p^{2m} = 0$ since $2m \geq n$. Since $4 \nmid p$, it follows that $d^2 = 0$ and hence $17bd^2 = 0$, $b^2d^2 = 0$ and $d^3 = 0$. The claim follows from Theorem 2.3.

2. $c \neq 0$. Suppose that $f(x)$ is self-invertible. Then by Theorem 2.3 we have that $a = -1$ and $b^2 + c = 0$. Since $c \neq 0$, $b \neq 0$. Then, by Proposition 3.1 we can write $b = up^k$, $c = vp^l$ for some units u, v and integers k, l such that $0 \leq k < n$ and $0 \leq l < n$. Thus,

$$0 = b^2 + c = u^2p^{2k} + vp^l. \tag{18}$$

If $2k < l$, then $0 = p^{2k}(u^2 + vp^{l-2k})$ with $u^2 + vp^{l-2k}$ a unit. Hence, $2k \geq n$ and therefore $b^2 = 0$ which is a contradiction since $c \neq 0$.
If $2k > l$, then $0 = p^l(u^2p^{2k-l} + v)$ with $u^2p^{2k-l} + v$ a unit. Hence, $l \geq n$ and therefore $c = vp^l = 0$, a contradiction.
Therefore, $2k = l$ and so $k < \frac{n}{2}$. Putting $l = 2k$ in relation (18) we obtain $0 = p^{2k}(u^2 + v)$ which implies that p^{n-2k} divides $(u^2 + v)$ since $2k < n$.

   (a) Suppose that $m < 3k$. Since $f(x)$ is self-invertible, by Theorem 2.3, $2b^4 - 3bd = 0$ and then $2u^4p^{4k} - 3uwp^{k+m} = 0$. Since $m < 3k$, $k+m < 4k$ and hence $p^{k+m}(2u^4p^{3k-m} - 3uw) = 0$ with $2u^4p^{3k-m} - 3uw$ a unit. It follows that $k+m \geq n$. On the other hand from Theorem 2.3, $4d^2+3b^3d = 0$ and then, $0 = 4w^2p^{2m} + 3u^3wp^{3k+m} = wp^{2m}(4w + 3u^3p^{3k-m})$ with $4w + 3u^3p^{3k-m}$ a unit since $m < 3k$. It follows that $2m \geq n$ and hence $m \geq \frac{n}{2}$.

   (b) Suppose that $m = 3k$. Since $f(x)$ is self-invertible, from Theorem 2.3 we have $0 = 2b^4 - 3bd = up^{4k}(2u^3 - 3w)$. If $4k < n$, then p^{n-4k} divides $(2u^3 - 3w)$. But from Theorem 2.3, $0 = 4d^2 + 3b^3d = p^{6k}w(4w + 3u^3)$. Suppose that $6k < n$. Then p divides $(2u^3-3w)$, p divides $(4w+3u^3)$ and hence p divides $-3(2u^3-3w)+2(4w+3u^3) = 17w$ which is a contradiction since $p > 17$ and w is a unit. Therefore, $6k \geq n$.

   (c) Suppose that $m > 3k$. Since $f(x)$ is self-invertible, from Theorem 2.3, $2b^4 - 3bd = 0$. Then $0 = up^{4k}(2u^3 - 3wp^{m-3k})$ with $2u^3 - 3wp^{m-3k}$ a unit since $m > 3k$. Therefore, $4k \geq n$ which is equivalent to $k \geq \frac{n}{4}$ and so $m > \frac{3n}{4}$.

Conversely, suppose that $f(x) = -x + up^k x^2 + vp^{2k} x^3 + wp^m x^4$ where $k < \frac{n}{2}$, u, v and w are units such that p^{n-2k} divides $(u^2 + v)$ and $m < n$. Then, $a = -1$, $b = up^k$, $c = vp^{2k}$, $d = wp^m$, and therefore $b^2 + c = p^{2k}(u^2 + v) = 0$.

(a) If $m < 3k$, $k + m \geq n$ and $\frac{n}{2} \leq m < n$. Then $n \leq k + m < 4k$. It is straightforward to see that all relations in Theorem 2.3 are satisfied, which implies that $f(x)$ is self-invertible.

(b) If $m = 3k$, $\frac{n}{6} \leq k < \frac{n}{4}$ and $p^{n-4k} \mid (2u^3 - 3w)$. Then, $m \geq \dfrac{n}{2}$. A direct calculation shows that all relations of Theorem 2.3 are satisfied, and hence $f(x)$ is self-invertible.

(c) If $m > 3k$ and $\frac{n}{4} \leq k < \frac{n}{2}$. Then $\frac{3n}{4} < m$. Again, it is easy to see that all relations of Theorem 2.3 are satisfied, and therefore $f(x)$ is self-invertible.

□

4 A relation with Strong Gröbner Bases

Some results will be presented on Gröbner bases associated to self-invertible cubic and quartic permutation polynomials discussed in Section 2. In order to prove these results we first recall some facts on Gröbner bases.

Throughout this section, R will denote a (commutative) principal ideal ring. The monoid of terms in $x_1, \ldots, x_n$ is denoted by T. We fix an admissible order "$<$" on T. If $f = \sum_{t \in T} f_t t \in R[x_1, \ldots, x_n] \setminus \{0\}$ and $v = \max\{t \in T \mid f_t \neq 0\}$ then v is called the *leading term*, f_v the *leading coefficient* and $f_v v$ the *leading monomial* of f, denoted $\mathrm{lt}(f)$, $\mathrm{lc}(f)$ and $\mathrm{lm}(f)$ respectively. If $S \subset R[x_1, \ldots, x_n] \setminus \{0\}$, we write $\mathrm{lm}(S)$ for $\{\mathrm{lm}(g) \mid g \in S\}$, and similarly for $\mathrm{lc}(S)$ and $\mathrm{lt}(S)$. Note that the terminology "leading term", "leading monomial", etc. differs from [1].

Let us recall the definition of a G-polynomial (see [2]).

Definition 4.1. *Let $F = \{f_1, \ldots, f_k\} \subset R[x_1, \ldots, x_n] \setminus \{0\}$. A G-polynomial of F is any polynomial $\sum_{i=1}^{k} c_i t_i f_i$ where $\sum_{i=1}^{k} c_i lc(f_i) \in gcd(lc(F))$, $c_i \in R$ and $t_i = \frac{lcm(lt(F))}{lt(f_i)}$. We write $Gpol(f)$ or $Gpol(f_1, \ldots, f_k)$ for the set of G-polynomials of $\{f_1, \ldots, f_k\}$.*

In [6] the following result (Lemma 5.7) was stated.

Let $F = \{f_1, \ldots, f_k\}$, $F' = \{f'_1, \ldots, f'_{k'}\}$ be subsets of $R[x_1, \ldots, x_n] \setminus \{0\}$ and let $h \in \mathrm{Gpol}(F)$, $h' \in \mathrm{Gpol}(F')$. Then

1. $\mathrm{Gpol}(h, h') = \mathrm{Gpol}(F \cup F')$.

2. If $k = k'$ and $\mathrm{lm}(f_i) \mid \mathrm{lm}(f'_i)$ for $i = 1, \ldots, k$, then $\mathrm{lm}(h) \mid \mathrm{lm}(h')$.

However, condition 1 is not true as the following example due to Eva Zerz shows ([10]). Consider $F = F' = \{x + 1, y + 1\}$ in $\mathbb{Z}[x, y]$, and $h = h' = xy + x$. Then, $\mathrm{Gpol}(h)$ consists only of h and $-h$, but $\mathrm{Gpol}(F)$ contains all the polynomials of the form $ay(x + 1) + (1 - a)x(y + 1)$ where $a \in \mathbb{Z}$; in particular it also contains $xy + y$.

This example shows that in general $\mathrm{Gpol}(F \cup F') \not\subset \mathrm{Gpol}(h, h')$. Next we prove that $\mathrm{Gpol}(h, h') \subset \mathrm{Gpol}(F \cup F')$ and $\mathrm{lm}(\mathrm{Gpol}(h, h')) = \mathrm{lm}(\mathrm{Gpol}(F \cup F'))$ which was pointed out to Ana Sălăgean by Eva Zerz ([7]). First we recall the definitions of Gpol-closed and Gpol-closure given in [6].

Definition 4.2. *Let G be a finite non-empty subset of $R[x_1, \ldots, x_n] \setminus \{0\}$. We say that*

1. *G is Gpol-closed if for all $g_i, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in Gpol(g_1, g_2)$ which is strongly reducible wrt. G.*

2. *G is a Gpol-closure of $G' \subseteq G$ if G is Gpol-closed and*

$$G \subseteq \bigcup_{\emptyset \neq F' \subseteq G'} Gpol(F'). \tag{19}$$

Lemma 4.3. *Let $F = \{f_1, \ldots, f_k\}$, $F' = \{f'_1, \ldots, f'_{k'}\}$ be subsets of $R[x_1, \ldots, x_n] \setminus \{0\}$ and let $h_1 \in Gpol(F)$, $h_2 \in Gpol(F')$. Then*

1. *$Gpol(h_1, h_2) \subset Gpol(F \cup F')$ and $lm(Gpol(h_1, h_2)) = lm(Gpol(F \cup F'))$.*

2. *If $k = k'$ and $lm(f_i)$ divides $lm(f'_i)$ for $i = 1, \ldots, k$, then $lm(h_1)$ divides $lm(h_2)$.*

Proof. 1. Let $g \in \mathrm{Gpol}(h_1, h_2)$. Then $g = c_1 t_1 h_1 + c_2 t_2 h_2$ where $h_1 \in \mathrm{Gpol}(F)$, $h_2 \in \mathrm{Gpol}(F')$, $t_i = \frac{\mathrm{lcm}(\mathrm{lt}_{(h_1)}, \mathrm{lt}_{(h_2)})}{\mathrm{lt}_{(h_i)}}$, $i = 1, 2$, and $c_1 lc(h_1) + c_2 lc(h_2) \in \gcd(lc(h_1), lc(h_2))$.

Since $h_1 \in \mathrm{Gpol}(F)$ and $h_2 \in \mathrm{Gpol}(F')$, we have $h_1 = \sum_{i=1}^{k} d_i s_i f_i$, $h_2 = \sum_{j=1}^{k'} d'_j s'_j f'_j$ where $\sum_{i=1}^{k} d_i lc(f_i) \in \gcd(lc(F))$, $\sum_{j=1}^{k'} d'_j lc(f'_j) \in \gcd(lc(F'))$, $s_i = \frac{\mathrm{lcm}(\mathrm{lt}_{(F)})}{\mathrm{lt}_{(f_i)}}$ for $i = 1, \ldots, k$ and $s'_j = \frac{\mathrm{lcm}(\mathrm{lt}_{(F')})}{\mathrm{lt}_{(f'_j)}}$ for $j = 1, \ldots, k'$. Then

$$g = c_1 \sum_{i=1}^{k} d_i t_1 s_i f_i + c_2 \sum_{j=1}^{k'} d'_j t_2 s'_j f'_j.$$

Now we show that $t_1 s_i = \frac{\mathrm{lcm}(\mathrm{lt}_{(F\cup F')})}{\mathrm{lt}_{(f_i)}}$ for $i = 1, \ldots, k$ and $t_2 s'_j = \frac{\mathrm{lcm}(\mathrm{lt}_{(F\cup F')})}{\mathrm{lt}_{(f'_j)}}$ for $j = 1, \ldots, k'$. Indeed, since $\mathrm{lt}(s_i f_i) = \mathrm{lcm}(\mathrm{lt}(F))$ and $\mathrm{lt}(s'_j f'_j) = \mathrm{lcm}(\mathrm{lt}(F'))$ we have $\mathrm{lm}(h_1) = lc(h_1) \cdot \mathrm{lcm}(\mathrm{lt}(F))$ and $\mathrm{lm}(h_2) = lc(h_2) \cdot \mathrm{lcm}(\mathrm{lt}(F'))$ where

$$lc(h_1) = \sum_{i=1}^{k} d_i lc(f_i) \quad \text{and} \quad lc(h_2) = \sum_{j=1}^{k'} d'_j lc(f'_j).$$

Then $\mathrm{lt}(h_1) = \mathrm{lcm}(\mathrm{lt}(F))$, $\mathrm{lt}(h_2) = \mathrm{lcm}(\mathrm{lt}(F'))$ and

$$\begin{aligned} t_1 s_i &= \frac{\mathrm{lcm}(\mathrm{lt}(h_1), \mathrm{lt}(h_2))}{\mathrm{lt}(h_1)} \cdot \frac{\mathrm{lcm}(\mathrm{lt}(F))}{\mathrm{lt}(f_i)} \\ &= \frac{\mathrm{lcm}(\mathrm{lcm}(\mathrm{lt}(F)), \mathrm{lcm}(\mathrm{lt}(F')))}{\mathrm{lcm}(\mathrm{lt}(F))} \cdot \frac{\mathrm{lcm}(\mathrm{lt}(F))}{\mathrm{lt}(f_i)} \\ &= \frac{\mathrm{lcm}(\mathrm{lt}(F \cup F'))}{\mathrm{lt}(f_i)} \end{aligned}$$

for $i = 1, \ldots, k$. Similarly we obtain $t_2 s'_j = \frac{\mathrm{lcm}(\mathrm{lt}_{(F\cup F')})}{\mathrm{lt}_{(f'_j)}}$ for $j = 1, \ldots, k'$.
On the other hand it is clear that $c_1 lc(h_1) + c_2 lc(h_2) \in \gcd(lc(F \cup F'))$ and therefore $g \in \mathrm{Gpol}(F \cup F')$. Thus $\mathrm{Gpol}(h_1, h_2) \subset \mathrm{Gpol}(F \cup F')$. In particular, $\mathrm{lm}(\mathrm{Gpol}(h_1, h_2)) \subset \mathrm{lm}(\mathrm{Gpol}(F \cup F'))$. Conversely, let $f \in \mathrm{lm}(\mathrm{Gpol}(F \cup F'))$. Then $f = \sum_{i=1}^{k} c_i t_i f_i + \sum_{j=1}^{k'} c'_j t'_j f'_j$ where

$$\mathrm{lm}(f) = \left(\sum_{i=1}^{k} c_i \mathrm{lc}(f_i) + \sum_{j=1}^{k'} c'_j \mathrm{lc}(f'_j) \right) \cdot \mathrm{lcm}(\mathrm{lt}(F \cup F')).$$

We must find $c_1^*, c_2^* \in R$ such that

$$\mathrm{lm}(f) = (c_1^* \mathrm{lc}(h_1) + c_2^* \mathrm{lc}(h_2)) \cdot \mathrm{lcm}(\mathrm{lt}(h_1), \mathrm{lt}(h_2)),$$

or

$$c_1^* \sum_{i=1}^{k} d_i lc(f_i) + c_2^* \sum_{j=1}^{k'} d'_j lc(f'_j) = \sum_{i=1}^{k} c_i lc(f_i) + \sum_{j=1}^{k'} c'_j lc(f'_j)$$

since $\mathrm{lt}(h_1) = \mathrm{lcm}(\mathrm{lt}(F))$ and $\mathrm{lt}(h_2) = \mathrm{lcm}(\mathrm{lt}(F'))$.
Let $C = \sum_{i=1}^{k} c_i lc(f_i) + \sum_{j=1}^{k'} c'_j lc(f'_j)$. We know that $C \in \gcd(\mathrm{lc}(F \cup F'))$, $\mathrm{lc}(h_1) \in \gcd(\mathrm{lc}(F))$ and $\mathrm{lc}(h_2) \in \gcd(\mathrm{lc}(F'))$. Let $D \in \gcd(\mathrm{lc}(h_1), \mathrm{lc}(h_2))$. Then $\langle C \rangle_R = \langle D \rangle_R$ and therefore $C = uD$ for some unit $u \in R$ by Proposition 4.1 of [6]. Now if $g = c_1^* s_1 h_1 + c_2^* s_2 h_2$ then $ug = u(c_1^* s_1 h_1 + c_2^* s_2 h_2)$ and $\mathrm{lc}(u^{-1} g) = u c_1^* \mathrm{lc}(h_1) + u c_2^* \mathrm{lc}(h_2) = uD$ which implies that $\mathrm{lm}(\mathrm{Gpol}(F \cup F')) \subset \mathrm{lm}(\mathrm{Gpol}(h_1, h_2))$.

2. Suppose that $k = k'$ and $\mathrm{lm}(f_i) \mid \mathrm{lm}(f'_i)$ for all $i = 1, \ldots, k$. Since $\mathrm{lm}(f_i) = \mathrm{lc}(f_i)\mathrm{lt}(f_i)$ and $\mathrm{lm}(f'_i) = lc(f'_i)\mathrm{lt}(f'_i)$ there exists $d_i \in R$ such that $\mathrm{lc}(f'_i)\mathrm{lt}(f'_i) = d_i\mathrm{lc}(f_i)\mathrm{lt}(f_i)$ for all $i = 1, \ldots, k$. Hence, $\mathrm{lc}(f_i) \mid \mathrm{lc}(f'_i)$ and $\mathrm{lt}(f_i) \mid \mathrm{lt}(f'_i)$ for all $i = 1, \ldots, k$.
As $\mathrm{lm}(h_1) = \mathrm{lc}(h_1)\mathrm{lcm}(\mathrm{lt}(F))$ and $\mathrm{lm}(h_2) = \mathrm{lc}(h_2)\mathrm{lcm}(\mathrm{lt}(F'))$, it follows that $\mathrm{lcm}(\mathrm{lt}(F)) \mid \mathrm{lcm}(\mathrm{lt}(F'))$. Similarly, $\mathrm{lc}(h_1) \mid \mathrm{lc}(h_2)$ since $\mathrm{lc}(h_1) \in \gcd(\mathrm{lc}(F))$ and $\mathrm{lc}(h_2) \in \gcd(\mathrm{lc}(F'))$. Thus, $\mathrm{lm}(h_1) \mid \mathrm{lm}(h_2)$.

□

The other results in [6] still hold but the proof of Proposition 5.8 requires revision. We recall the definitions of reduction and strong reduction.

Definition 4.4. *Let A be a commutative ring with $1 \neq 0$. Let $f \in A[x_1, \ldots, x_n] \setminus \{0\}$ and let G be a finite, non-empty subset of $A[x_1, \ldots, x_n] \setminus \{0\}$.*

1. *We say that f reduces to h with respect to G in one step (and that f is reducible with respect to G) if $h = f - \sum_{i=1}^{k} c_i t_i g_i$, where $c_i \in A$, $t_i \in T$, $g_i \in G$, $lm(f) = \sum_{i=1}^{k} c_i t_i lm(g_i)$ and $c_i \neq 0$ implies $c_i lc(g_i) \neq 0$ and $lt(f) = t_i lt(g_i)$. We write this as $f \to_G h$.*

2. *We say that f strongly reduces to h wrt. G in one step (and that f is strongly reducible wrt. G) if $h = f - mg$ where $g \in G$ and m is a monomial such that $lm(f) = m \cdot lm(g)$. We write this as $f \twoheadrightarrow_G h$.*

3. *The reflexive and transitive closures of the relations $\to_G$ and $\twoheadrightarrow_G$ are denoted $\to_G^*$ and $\twoheadrightarrow_G^*$ respectively. When $f \to_G^* h$ we say that f reduces to h wrt. G. Similarly for the strong reduction.*

Proposition 4.5. *Let $G, G' \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be finite sets satisfying condition (19). The following assertions are equivalent:*

1. *G is a Gpol-closure of G'.*

2. *For all non-empty $F' \subseteq G'$, there is an $h \in Gpol(F')$ which is strongly reducible wrt. G.*

3. *For all non-empty $F' \subseteq G'$ such that $lt(F')$ is saturated wrt. $lt(G')$, there is an $h \in Gpol(F')$ which is strongly reducible wrt. G.*

4. *For all $f \in R[x_1, \ldots, x_n]$, f is reducible wrt. G' if and only if f is strongly reducible wrt. G.*

Proof. We need only change the proof of (2) ⇒ (1). The rest of the proof is the same given in Proposition 5.8 of [6].
We need only show that G is Gpol-closed, so let $h_1, h_2 \in G$ with $h_1 \neq h_2$. From

condition (19), there are F'', $F' \subseteq G'$ such that $h_1 \in \mathrm{Gpol}(F')$ and $h_2 \in \mathrm{Gpol}(F'')$. By (2), there is an $h \in \mathrm{Gpol}(F' \cup F'')$ which is strongly reducible wrt. G. Suppose that h strongly reduces to h' wrt. G in one step, say $h' = h - mg$ for some $g \in G$ and m is a monomial such that $\mathrm{lm}(h) = m \cdot \mathrm{lm}(g)$. By Lemma 4.3, $\mathrm{lm}(h) = \mathrm{lm}(f)$ for some $f \in \mathrm{Gpol}(h_1, h_2)$. Then f strongly reduces to $f' = f - mg$ wrt. G in one step and therefore f is strongly reducible wrt. G. □

It should be noted that with the modification in Lemma 4.3 the claims of Proposition 5.10 and its consequences, particularly Corollary 5.13 of [6] still hold.

We end this note by giving a relationship between Gröbner bases and the equations on the coefficients of quartic and cubic permutation polynomials given in Theorem 2.3 and Remark 2.4 respectively, which characterize when these polynomials are self-invertible. Before to state these claims we recall the following concepts.

Definition 4.6.

1. *Let $g_1, g_2 \in R[x_1, ..., x_n]$ be non-zero distinct polynomials. An S-polynomial of g_1 and g_2 is any polynomial $c_1 t_1 g_1 - c_2 t_2 g_2$ where,*

$$c_1 lc(g_1) - c_2 lc(g_2) \in lcm(lc(g_1), lc(g_2)) \neq \{0\}$$

   $c_i \in R$ and $t_i = lcm(lt(g_1), lt(g_2))/lt(g_i)$. The set of all S-polynomials of g_1, g_2 will be denoted by $Spol(g_1, g_2)$.

2. *An A-polynomial of $0 \neq g \in R[x_1, ..., x_n]$ is any polynomial of the form ag where $a \in R$ is such that $\langle a \rangle_R = Ann(lc(g))$. The set of all A-polynomials of g will be denoted by $Apol(g)$.*

Theorem 4.7. *Let p be a prime and n be a positive integer. The set*

$$G = \{a + 1, b^2 + c, c^2\}$$

is a strong Gröbner basis for the ideal $I = \langle G \rangle$ in $\mathbb{Z}_{p^n}[a, b, c]$ with the lexicographic order $b > c > a$.

Proof. Since the ring $\mathbb{Z}_n$ is a finite-chain ring, we may apply Corollary 5.13 of [6]. We must show that
(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow_G^* 0$ and;
(B) for any $g \in G$ there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow_G^* 0$.
In order to check condition (A), from the definition of S-polynomial, given $g_1, g_2 \in G$ we have to find an h of the form $c_1 t_1 g_1 - c_2 t_2 g_2$ such that $c_1 \mathrm{lc}(g_1) = c_2 \mathrm{lc}(g_2) \in$

$\mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) \neq \{0\}$ where $c_i \in \mathbb{Z}_{p^n}$ and $t_i = \frac{\mathrm{lcm}(\mathrm{lt}_{(g_1)}, \mathrm{lt}_{(g_2)})}{\mathrm{lt}_{(g_i)}}$ for $i = 1, 2$. Also we need to show that $h \twoheadrightarrow_G^* 0$.
If $g_1 = a + 1$ and $g_2 = b^2 + c$, then $\mathrm{lcm}(a, b^2) = ab^2$, $t_1 = b^2$ and $t_2 = a$. Hence, $h = b^2(a + 1) - a(b^2 + c) = b^2 - ac \twoheadrightarrow_G -c(a + 1) \twoheadrightarrow_G 0$, that is $h \twoheadrightarrow_G^* 0$.
If $g_1 = a + 1$ and $g_2 = c^2$, then $\mathrm{lcm}(a, c^2) = ac^2$, $t_1 = c^2$ and $t_2 = a$. Hence, $h = c^2(a + 1) - a(c^2) = c^2 \twoheadrightarrow_G^* 0$.
If $g_1 = b^2 + c$ and $g_2 = c^2$, then $\mathrm{lcm}(b^2, c^2) = b^2c^2$, $t_1 = c^2$ and $t_2 = b^2$. Hence, $h = c^2(b^2 + c) - b^2(c^2) = c^3 \twoheadrightarrow_G^* 0$.
In all cases above it is clear that $c_1\mathrm{lc}(g_1) = c_2\mathrm{lc}(g_2) \in \mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) \neq \{0\}$.
Now, condition (B) is easy to check. This completes the proof. □

Theorem 4.8. *Let $p > 3$ be a prime and n be a positive integer. The set*

$$G = \{a + 1, c + b^2, 2b^4 - 3bd, 3b^3d + 4d^2, 17bd^2, b^2d^2, d^3\}$$

is a strong Gröbner basis for the ideal $I = \langle G \rangle$ in $\mathbb{Z}_{p^n}[a, b, c, d]$ with the lexicographic order $c > b > d > a$.

Proof. As in the proof of Theorem 4.7 we must verify the following two conditions.
(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow_G^* 0$ and;
(B) for any $g \in G$ there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow_G^* 0$.
Since we have to verify condition (A) for 21 distinct pairs of elements of G, we simply check it for some pairs and the rest can be checked in a similar way.
Given $g_1, g_2 \in G$ we have to find an h of the form $c_1t_1g_1 - c_2t_2g_2$ such that $c_1\mathrm{lc}(g_1) = c_2\mathrm{lc}(g_2) \in \mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) \neq \{0\}$ where $c_i \in \mathbb{Z}_{p^n}$ and $t_i = \frac{\mathrm{lcm}(\mathrm{lt}_{(g_1)}, \mathrm{lt}_{(g_2)})}{\mathrm{lt}_{(g_i)}}$ for $i = 1, 2$. Also we need to show that $h \twoheadrightarrow_G^* 0$.
Let's consider the elements $g_1 = 2b^4 - 3bd$ and $g_2 = 3b^3d + 4d^2$. Since $\mathrm{lcm}(b^4, b^3d) = b^4d$ we have that $t_1 = d$ and $t_2 = b$. Thus, putting $h = 3d(2b^4 - 3bd) - 2b(3b^3d + 4d^2) = -9bd^2 - 8bd^2 = -17bd^2$ it follows that h strongly reduces to 0 wrt. G in one step and therefore $h \twoheadrightarrow_G^* 0$.
Now if, for example, $g_1 = c + b^2$ and $g_2 = 2b^4 - 3bd$, then $\mathrm{lcm}(c, b^4) = cb^4$, $t_1 = b^4$ and $t_2 = c$. Thus, $h = 2b^4(c + b^2) - c(2b^4 - 3bd) = 3cbd + 2b^6$ strongly reduces to 0 wrt. G since $h \twoheadrightarrow_G 2b^6 - 3b^3d \twoheadrightarrow_G 0$.
As a final example, suppose that $g_1 = c + b^2$ and $g_2 = 3b^3d + 4d^2$. Then, $\mathrm{lcm}(c, b^3d) = cb^3d$, $t_1 = b^3d$ and $t_2 = c$. Thus, $h = 3b^3d(c + b^2) - c(3b^3d + 4d^2) = -4cd^2 + 3b^5d$ strongly reduces to 0 wrt. G since $h \twoheadrightarrow_G 3b^5d + 4b^2d^2 \twoheadrightarrow_G (4 + 9 \cdot 2^{-1})b^2d^2 \twoheadrightarrow_G 0$.
Observe that in the previous examples the condition

$$c_1\mathrm{lc}(g_1) = c_2\mathrm{lc}(g_2) \in \mathrm{lcm}(\mathrm{lc}(g_1), \mathrm{lc}(g_2)) \neq \{0\}$$

is satisfied.
Now, condition (B) is easy to check and the proof is completed. □

Acknowledgments

We thank Ana Sălăgean and Eva Zerz for their helpful observations on Gröbner bases over principal ideal rings.

References

[1] W. Adams, P. Loustaunau. *An Introduction to Gröbner bases*, Volume 3 of Graduate Studies in Mathematics. American Mathematical Society, 1994. http://dx.doi.org/10.1090/gsm/003

[2] T. Becker, V. Weispfenning. *Gröbner Bases*. Graduate Texts in Mathematics 141. Springer, 1993. http://dx.doi.org/10.1007/978-1-4612-0913-3

[3] J. Diaz-Vargas, C.J. Rubio-Barrios, J.A. Sozaya-Chan and H. Tapia-Recillas, *Self-Invertible Quadratic (Cubic) Permutation Polynomials over* $\mathbb{Z}_{2^n}$ *(*$\mathbb{Z}_{p^n}, p >$ 7*)*, Int. J. Algebra, Vol. 6, 2012, no. 17, 863-874.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge University Press, 2003.

[5] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.

[6] G. H. Norton, A. Sălăgean, *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. Vol. 64 (2001), 505-528. http://dx.doi.org/10.1017/s0004972700019973

[7] A. Sălăgean, *Personal Correspondence with Carlos J. Rubio*, 2013.

[8] Y. O. Takeshita, *Interleavers for turbo codes using permutation polynomials over integer rings*, IEEE Trans. Inf. Theory, vol.51, no.1, pp.101-119, (2005). http://dx.doi.org/10.1109/tit.2004.839478

[9] H. Tapia-Recillas, *Remarks on Self-Inverse Quadratic Permutation Polynomials*, Int. J. Algebra, Vol. 4, no. 19, 931-938 (2010).

[10] E. Zerz, *Personal Correspondence with Carlos J. Rubio*, 2013.

Received: March 2, 2015; Published: March 27, 2015