International Journal of Algebra, Vol. 12, 2018, no. 7, 285 - 295
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.8935

On Permutation Polynomials over Local Finite Commutative Rings

Javier Diaz-Vargas

Universidad Autónoma de Yucatán, Facultad de Matemáticas, Periférico Norte
Tablaje 13615, 97203, Mérida, Yucatán, México

José Antonio Sozaya-Chan

Departamento de Matemáticas, Universidad Autónoma Metropolitana
Unidad Iztapalapa, 09340, Ciudad de México, México

Abstract

In this paper, we give criteria for a polynomial to be a permutation polynomial of a local finite commutative ring with identity. These criteria generalize known results established for finite fields.

On the other hand, we also study the permutation polynomials on this type of rings that are self-invertible.

Mathematics Subject Classification: 13H99, 13M10

Keywords: Local finite commutative rings, permutation polynomials, self-invertible permutation polynomials

1 Introduction

Permutations play an important role in areas of transmission and information security, for example in the design of some encryption algorithms and in the design of the so-called S-boxes [7]. They are also important in error-correcting codes.

We must generate such permutations in an agile manner. One way to do this is through the so-called permutation polynomials.

Let R be a finite commutative ring. A polynomial $f(x)$ with coefficients in R is said to be a *permutation polynomial of* R if the induced function $f : c \mapsto f(c)$ from R to itself is a bijection, that is, if f is a permutation on R.

For the most part, these polynomials have been studied on finite fields. In this context, recent applications of them can be found in [8].

In this paper, we use some criteria for a polynomial to be a permutation polynomial to generalize to local finite commutative rings some known results for finite fields.

For some applications, for certain given permutation, it is important to determine its inverse and that this inverse can be found efficiently from the computational point of view. For example, self-invertible permutation polynomials are convenient since no additional work is required to determine their inverse. Here, we characterize the null polynomials in local finite commutative rings and use these polynomials to give conditions for a polynomial to be self-invertible in this class of rings. This generalizes the results found in [1] for the local rings $\mathbb{Z}_{p^n}$.

Let us fix the notation to be used. From now on,

- R will denote a finite local commutative ring with identity.
- The maximal ideal of R is denoted by $\mathfrak{m} \neq 0$.
- The residue field is $F = R/\mathfrak{m}$ of order $q = p^\delta$, where p is a prime number.
- Let $^- : R \to F$ be the canonical projection that sends each element to its residue class module $\mathfrak{m}$.

Note that R is not a finite field, since its maximal ideal $\mathfrak{m} \neq 0$.

2 Criteria for permutation polynomials

Because of the finiteness of R, the definition of a permutation polynomial can be expressed in several equivalent ways:

1. $f(x)$ is a permutation polynomial of R;
2. the function f from R into R induced by $f(x)$ is one-to-one or onto;
3. for every $a \in R$, the equation $f(z) = a$ has a solution in R.

Remark 2.1. *The linear coefficient of a permutation polynomial of R is a unit since $\mathfrak{m}$ is a nilpotent ideal, this fact follows, in a simple way, from Nakayama's lemma [6, p. 84]; indeed, if its nilpotency index is $n \geq 2$ and if*

$$f(x) = ax + x^2 g(x)$$

is in $R[x]$ with $a \in \mathfrak{m}$, then $f(\mathfrak{m}^{n-1}) = 0$ but $\mathfrak{m}^{n-1} \neq 0$. Thus, if $f(x)$ is a permutation polynomial, then $a \notin \mathfrak{m}$ and so, a is a unit.

Theorem 2.2. *A polinomial $ax + x^2 g(x)$ in $R[x]$ with $a \in R^*$ is a permutation polynomial of R if and only if the induced function permutes the units of R.*

Proof. Let $f(x) = ax + x^2 g(x)$ as above. Then

$$f(x) - f(y) = (x - y)[a + h(x, y)\,] \tag{1}$$

for some polynomial $h(x, y)$ in two indeterminates over R with constant term zero.

Assume that f permutes the units of R. Since $R^* = R \setminus \mathfrak{m}$, to prove that $f(x)$ is a permutation polynomial it is suffices to show that f permutes the elements of the maximal ideal $\mathfrak{m}$. Let $b, c \in \mathfrak{m}$ such that $f(b) = f(c)$. Since $d = h(b, c)$ is in $\mathfrak{m}$ and a is a unit, its sum $a + d$ is also a unit and therefore, from (1) it follows that $b = c$. This proves the sufficiency.

To prove the necessity, we note that $f(\mathfrak{a}) \subseteq \mathfrak{a}$ for any ideal $\mathfrak{a}$ of R. So if f is a permutation on R then $f(\mathfrak{m}) = \mathfrak{m}$ by finiteness. Thus f permutes the units of R. □

The following lemma is useful in the proof that we present of the established criterion in [4, Proposition 4.34, p. 165]. For another approach see [3, Theorem 3.3, p. 205]

First, we extend the canonical projection of the ring R to the polynomial ring $R[x]$ in the natural way: for $g(x) = a_0 + a_1 + \cdots + a_n x^n$ we let $\overline{g}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n$.

Lemma 2.3. *If $g(x)$ is a regular polynomial in $R[x]$ and $c \in F$ is a simple root of $\overline{g}(x)$, then $g(x)$ has one and only one root $a \in R$ such that $\overline{a} = c$.*

Proof. See [6, Lemma XV.1, p. 292]. □

With respect to Lemma 2.3, if $c \in F$ is a multiple root of $\overline{g}(x)$, the situation is somewhat different as shown in [6, pp. 269-271]. In this case, if there exists such root $a \in R$ of $g(x)$ with the property $\overline{a} = c$, then it is not unique.

Example 2.4. *Let $n \geq 1$ be a divisor of $q-1$. The equation $z^n = 1$ has exactly n solutions in R by Lemma 2.3, because $x^n - 1$ is a binomial with precisely n roots in F and all them are simple roots according to the derivative criterion. In particular, if q is odd the only solutions in R of the equation $z^2 = 1$ are ± 1.*

Theorem 2.5. *A polynomial $g(x)$ in $R[x]$ is a permutation polynomial of R if and only if the following two conditions simultaneously hold:*

1. *$\overline{g}(x)$ is a permutation polynomial of F;*

2. *the formal derivative $\overline{g}'(x)$ does not vanish on F.*

Proof. For simplicity, for every $a \in R$ we let $g_a(x) = g(x) - a$.

Suppose first that $g(x)$ is a permutation polynomial of R. Condition (a) holds since for every $c \in R$ we have that $\overline{g}(\overline{c}) = \overline{g(c)}$, so that $\overline{g}$ permutes the elements of F. On the other hand, in accordance to the discussion after Lemma 2.3, if $\overline{g}'(x)$ has a root $\overline{c} \in F$, then the number of roots of $g_c(x)$ in R is either zero or at least two, which is impossible since each $g_c(x)$ has exactly one root in R. Thus, condition (b) is satisfied.

Conversely assume that both conditions (a) and (b) hold. Hence, every $\overline{g}_c(x)$ has an only root in F which is simple by the derivative criterion. From here, Lemma 2.3 implies that every polynomial $g_c(x)$ has a root in R and so, g is onto. This ends the proof. □

2.1 Some examples of permutation polynomials

An immediate consequence of Theorem 2.5 is the following result that allows to obtain new permutation polynomials from one given by adding nilpotent monomials.

Corollary 2.6. *Let $f(x)$ be a permutation polynomial of R. Then*

$$h(x) = f(x) + \sum_{n=0}^{m} b_n x^n$$

is also a permutation polynomial of R provided that $b_0, \ldots, b_m$ all lie in $\mathfrak{m}$.

Proof. It follows from the fact that $\overline{b}_0, \ldots, \overline{b}_m$ in F are all zero. □

Next we give some examples of criteria for permutation polynomials over finite fields that generalize to finite local commutative rings by using Theorem 2.5. For this we only need to consider the formal derivatives.

Example 2.7. *Let $a \in R^*$. In $R[x]$, consider the p-polynomial*

$$g(x) = ax + \sum_{n=1}^{k} c_n x^{p^n},$$

where p is the characteristic of F. Since $\overline{g}'(x) = \overline{a} \neq 0$, Theorem 2.5 implies that $g(x)$ is a permutation polynomial of R if and only if $\overline{g}(x)$ is a permutation polynomial of F; but this amounts to the fact that the only root of $\overline{g}(x)$ in F is zero according to [5, Theorem 7.9, pp. 351].

Example 2.8. *Let $a \in R^*$ and let $k \geq 1$ be an integer. The* Dickson polynomial

$$g_k(x,a) = \sum_{n=0}^{[k/2]} \frac{k}{k-n} \binom{k-n}{n} (-a)^n x^{k-2n}$$

is a permutation polynomial of R if and only if $(k, pq^2 - p) = 1$. This is a consequence of a result in [4, Theorem 9.43, pp. 209], which states that $\overline{g_k}(x,a)$ is a permutation polynomial of F if and only if $(k, q^2 - 1) = 1$, and that when this occurs its formal derivative does not vanish on F if and only if k is no divisible by the characteristic p of F.

Example 2.9. *Let $a \in R^*$. If the characteristic p of F is different from 2, then $ax + x^{(q+1)/2}$ is a permutation binomial of R if and only if $\overline{a}^2 = d^2 + 1$ for some $d \in F^*$ and $2\overline{a} \neq \pm 1$. Indeed, $\overline{a}x + x^{(q+1)/2}$ is a permutation binomial of F if and only if $\overline{a}^2 - 1$ is a square in F^*, see [5, Theorem 7.11, p. 352]. On the other hand, its formal derivative $\overline{a} + 2^{-1}x^{(q-1)/2}$ has a root in F if and only if $2\overline{a} = \pm 1$. To see this we recall that every $c \in F^*$ satisfies $c^{q-1} = 1$; so that $c^{(q-1)/2}$ is a solution of $z^2 = 1$ and therefore it is either 1 or -1 in accordance to Example 2.4.*

Further examples can be obtained by formal composition of polynomials.

We say that a finite local commutative ring S is a *finite local extension* of R when it contains R as a subring.

Lemma 2.10. *If the field K is a finite extension of the field F, then K is the residue field of a finite local extension S of R.*

Proof. The K field is a primitive extension of the field F, that is, $K = F(a)$, where a is a root of an irreducible monic polynomial $\overline{f}$ in $F[x]$. Then its monic uplift $f \in R[x]$ is irreducible basic and $S = R[x]/(f)$ is a local finite commutative ring containing R [6, Corollary XIV.10, p. 289]. Now, S is R-free and

$$\deg f = \dim_R S = \dim_F K' = \deg \overline{f},$$

where K' is the residue field of S [6, p. 295]. From here, $K' \cong K$. □

Theorem 2.11. *A polynomial $f(x)$ in $R[x]$ is a permutation polynomial of all finite local extensions of R if and only if it is of the form*

$$f(x) = c + ax + \sum_{n=2}^{m} c_n x^n,$$

where a is a unit and $c_1, \ldots, c_m$ all lie in $\mathfrak{m}$.

Proof. The sufficiency is an immediate consequence of Corollary 2.6.

Before proving the necessity it should be noted the following. Let S be a finite local ring with residue field K and suppose $R \subseteq S$. Then, the maximal ideal of R is contained in the maximal ideal of S because every member of $\mathfrak{m}$ is a nilpotent element of R, and therefore, of S. This ensures the existence of a monomorphism from F into K, which is defined in the obvious way. So, we can think in an inclusion $F \subseteq K$.

Now we are ready to complete the proof. Let $f(x)$ be a permutation polynomial of all finite local extensions of R. Therefore, by condition (a) of Theorem 2.5 and by Lemma 2.10 above, $\overline{f}(x)$ is a permutation polynomial of all finite extensions of F. So, there is $a \in R^*$ such that

$$\overline{f}(x) = \overline{a}x^{p^k} + \overline{c},$$

for some integer $k \geq 0$. This claim is proven in [5, Theorem 7.14, p. 354] for arbitrary finite fields.

However, the linear coefficient of $f(x)$ must be a unit by Remark 2.1. Thus $k = 0$. □

It is well-known that

$$\sum_{a \in F} a^m = \begin{cases} 1 & \text{if } q-1 \text{ divides } m; \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Theorem 2.12. *Let $d > 1$ be a divisor of $q-2$ and let $dk = q-2$. If p does not divide $k+1$ then no binomial $ax + x^d$ in $R[x]$ is a permutation binomial of R.*

Proof. Let $f(x) = ax + x^d$ and by contraposition, assume that it is a permutation binomial of R. Therefore $\overline{a} \neq 0$ by Remark 2.1 and hence, condition (a) of Theorem 2.5 implies that $\overline{f}(x)$ is a permutation binomial of F.

Next, property (2) yields

$$\sum_{c \in F} \overline{f}(c)^{\,k+1} = \sum_{c \in F} \left[\, \overline{a}c + c^d \right]^{k+1} = 0 \tag{3}$$

because the induced function $\overline{f}$ permutes the elements of F and $(q-1) \nmid (k+1)$. By contradiction, suppose that $q-1$ divides to $k+1, (q-1)t = k+1$. Then,

since $dk+1 = q-1, (dk+1)t = k+1$. This implies that $k(dt-1)+(t-1) = 0$. If $t = 1$ then $d = 1$, a contradiction. If $t > 1$, then $k(dt-1) > 0$ and $t-1 > 0$ and there is no way that the sum is zero.

Now, given an integer n such that $0 \leq n \leq k+1$, we denote $m = (n-1)(d-1)$. We claim that $q-1$ divides m if and only if $n = 1$. Indeed, we have $|m| \leq q-2$ since $dk = q-2$; from here, $q-1$ divides m if and only if $m = 0$. But as $d > 1$, we deduce that $m = 0$ if and only if $n = 1$. From (2), we obtained

$$\sum_{c \in F} c^{dk+d-nd+n} = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{otherwise,} \end{cases}$$

since $d - nd + n = 1 - m$. This together with (3) yields $(k+1)\overline{a} = 0$ after expanding the binomials and changing the order of the sums. So, as $\overline{a} \neq 0$ we get $k+1 = 0$ as element of F, that is, as integer, $k+1$ is divisible by p. □

Remark 2.13. *Theorem 2.12 also holds for finite fields and its proof is essentially the same.*

3 Null polynomials

A polynomial $f(x)$ with coefficients in A is called *null polynomial* of A if $f = 0$; that is, if the associated polynomial function is the zero function, $f(a) = 0$ for every $a \in A$.

Example 3.1. *The null polynomials of a finite field K of order q are precisely, by the division algorithm, those polynomials in $K[x]$ which are divisible by the binomial $x^q - x$ of degree q.*

Lemma 3.2. *If $f(x)$ is a null polynomial of R of degree less than q, then $f(x) = 0$.*

Proof. Let $a_0, \ldots, a_{q-1}$ be q elements in R such that $\overline{a}_i \neq \overline{a}_j$ when $i \neq j$ and let $f(x)$ be a polynomial in $R[x]$ which vanishes in $a_0, \ldots, a_{q-1}$. Then, by the remainder theorem, every $x - a_j$ divides $f(x)$. We claim that $f(x)$ is also divisible by

$$u(x) = \prod_{j=0}^{q-1} (x - a_j)$$

in $R[x]$. This can be proved inductively since if

$$f(x) = \prod_{j=0}^{k-1} (x - a_j) h(x)$$

for some integer k with $1 \leq k \leq q-1$ then $f(a_k) = 0$ implies $h(a_k) = 0$ because $a_k - a_j$ is a unit when $j < k$, and therefore, $x - a_k$ divides $h(x)$.

Now, suppose that $f(x)$ is a null polynomial of R of degree less than q. Then $f(x)$ is divisible by the monic polynomial $u(x)$ of degree q. So, $f(x) = 0$. □

We next give a characterization of null polynomials of R when the only maximal ideal of R is a principal ideal, say $\mathfrak{m} = (e)$. This generalizes a result in [2, Theorem 27, p. 22]. We will give a proof along the lines of the mentioned theorem.

Theorem 3.3. *Let $\mathfrak{m} = (e)$ with nilpotency index n. Then, a polynomial $f(x)$ in $R[x]$ is a null polynomial of R if it is expressible as*

$$f(x) = \sum_{j=1}^{n} e^{n-j}(x^q - x)^j f_j(x) \tag{4}$$

where the $f_j(x)$ are in $R[x]$. The converse is true when $n < q$.

Proof. The first assertion is trivial since e divides $d^q - d$ for every $d \in R$ and $e^n = 0$.

On the other hand, we assume that $n < q$ and prove that if $f(x)$ is a null polynomial of R then it is of the form (4). We proceed by induction on nilpotency index of $\mathfrak{m}$. The case $n = 1$, which corresponds to finite fields, was discussed in the Example 3.1. Next, we suppose that assertion is true for $n-1$, with $1 < n < q$.

Let $S = R/\mathfrak{m}^{n-1}$. Hence, S is a finite local ring and its maximal ideal $\mathfrak{m}/\mathfrak{m}^{n-1}$ is a principal ideal with nilpotency index $n-1$. The induction hypothesis implies

$$f(x) = \sum_{j=1}^{n-1} e^{n-1-j}(x^q - x)^j f_j(x) + e^{n-1}h(x) \tag{5}$$

in $R[x]$, as one can see by lifting the corresponding expression (4) from $S[x]$ to $R[x]$.

Now, let $a \in R$. Then there is $c \in R$ such that $a^q - a = ec$. So,

$$(a + ex)^q - (a + ex) = e(c - x) + e^2 r(x)$$

for some $r(x)$ in $R[x]$. Hence, for any $1 \leq i \leq n-1$, we get

$$e^{n-1-i}\big[(a + ex)^q - (a + ex)\big]^i = e^{n-1}(c - x)^i.$$

By replacing x by $a+ex$ in (5), we obtain

$$f(a+ex) = \sum_{j=1}^{n-1} e^{n-1}(c-x)^j f_j(a+ex) + e^{n-1}h(a+ex)$$
$$= e^{n-1}\Big[\sum_{j=1}^{n-1}(c-x)^j f_j(a) + h(a)\Big]$$

and thus, replacing x by $c-x$, we conclude

$$f(a+e(c-x)) = e^{n-1}\Big[\sum_{j=1}^{n-1} x^j f_j(a) + h(a)\Big] = 0$$

by Lemma 3.2 since this polynomial is also a null polynomial of R but its degree is less than q. Consequently, $h(a)$ and every $f_j(a)$ are divisible by e for every $a \in R$ because a was arbitrarily chosen. From here, we can deduce that $\overline{h}(x)$ as well as each $\overline{f_j}(x)$ are null polynomials of F. Therefore, in $R[x]$ we have

$$f_j(x) = (x^q - x)s_j(x) + ek_j(x),$$

and in a similar way,

$$e^{n-1}h(x) = e^{n-1}(x^q - x)k(x).$$

The induction is completed by replacing this in (5) and then relabeling terms. □

4 Self-invertible permutation polynomials

A permutation polynomial $f(x)$ of R is said to be *self-invertible* if the permutation f that it induces on R has order 2, that is, if the inverse of f is itself.

Given a polynomial $f(x)$ in $R[x]$ we associate it with the polynomial

$$f_*(x) = f \circ f(x) - x,$$

where the symbol $\circ$ indicates formal composition of polynomials.

Remark 4.1. *If $f(x)$ is a self-invertible permutation polynomial of R of degree less than $\sqrt{q}$ then, as consequence of Lemma 3.2, $f_*(x) = 0$.*

Theorem 4.2. *Let $g(x) = ax + bx^m + x^{m+1}h(x)$ be a self-invertible permutation polynomial of R of degree $n < \sqrt{q}$, with $b \neq 0$ and $m > 1$. Then, except for a, all coefficients of $g(x)$ lie in $\mathfrak{m}$. Also, $a^2 = 1$ and if $2b \neq 0$ then m is even and $a \neq 1$.*

Proof. By Remark 4.1, $g_*(x) = 0$ and thus, $\overline{g}_*(x) = 0$. This implies that $\overline{g}(x)$ has degree 1 and proves the first claim.

On the other hand, it is not hard to see that

$$g_*(x) = (a^2 - 1)x + ab(1 + a^{m-1})x^m + x^{m+1}k(x),$$

so that $a^2 = 1$. Finally, if $a = 1$ or if m is odd, then $a^{m-1} = 1$ and, hence, $2b = 0$. □

Corollary 4.3. *Suppose $p \neq 2$ and let $g(x) = ax + bx^n$ be a self-invertible permutation binomial of R of degree $n < \sqrt{q}$. Then n is even, $a = -1$ and $nb^2 = 0$.*

Proof. From Theorem 4.2 it follows that $a^2 = 1$, n is even and $a \neq 1$ since $2b \neq 0$. Here we have used the fact that $2 \in R$ is a unit. Hence $a = -1$ by Example 2.4. Therefore,

$$g_*(x) = -b^2x^{2n-1}\,[\,n - bx^{n-1}h(x)\,],$$

which implies $nb^2 = 0$ because of $g_*(x) = 0$ by Remark 4.1. This ends the proof. □

Example 4.4. *Every permutation polynomial of R of the form*

$$f(x) = -x + \sum_{n=2}^{m} c_n x^{2n}$$

with $c_2, \ldots, c_m$ such that $c_r c_s = 0$ for all r, s is self-invertible since $f_*(x) = 0$.

Theorem 4.5. *A permutation polynomial $ax + bx^2 + cx^3$ of R is self-invertible provided that $a = -1$, $c = -b^2$ and $c^2 = 0$. The converse holds when q is odd and $q > 9$.*

Proof. Let $f(x) = ax + bx^2 + cx^3$. The first claim is straightforward since

$$\begin{aligned} f_*(x) = (a^2 - 1)x &+ ab(1 + a)x^2 + a(a^2c + 2b^2 + c)x^3 \\ &+ b(b^2 + 2ac + 3a^2c)x^4 + c(2b^2 + 3ab^2 + 3a^2c)x^5 \\ &+ bc(c + 6ac + b^2)x^6 + 3c(b^2 + ac)x^7 + 3bc^3x^8 + c^3x^9. \end{aligned}$$

Next, we assume that q is odd and $q < n^2$, where n is the degree of $ax + bx^2 + cx^3$. We will prove that if f is a permutation on R of order 2, then $a = -1$, $c = -b^2$ and $c^2 = 0$. Without loss of generality, we also suppose $n > 1$. First note that $f_*(x) = 0$ by Remark 4.1, so that $a^2 = 1$. Now, as $2a$ is a unit, from $a(a^2c + 2b^2 + c) = 0$, we get $b^2 = -c$; meanwhile from $ab(1 + a) = 0$, it follows that $a = -1$ by Example 2.4 since $a = 1$ implies $b = 0$ and so $c = 0$, a contradiction. Finally, by replacing this in $c(2b^2 + 3ab^2 + 3a^2c) = 0$, we obtain $c^2 = 0$. □

References

[1] J. Díaz-Vargas, C. Rubio-Barrios, J.A. Sozaya-Chan and H. Tapia-Recillas, Self-invertible quadratic (cubic) permutation polinomials over $\mathbb{Z}_{2^n}$ ($\mathbb{Z}_{p^n}$, $p > 7$), *International Journal of Algebra*, **6** (2012), no. 17, 863-874.

[2] L. Dickson, *Introduction to the Theory of Numbers*, Dover Publications, New York, 1957.

[3] D. Görcsös, G. Horváth, A. Mészáros, Permutation polynomials over finite rings, *Finite Fields and their Applications*, **49** (2018), 198-211. https://doi.org/10.1016/j.ffa.2017.10.004

[4] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North Holland, Amsterdan, 1973.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1996. https://doi.org/10.1017/cbo9780511525926

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

[7] A. J. Menezes, P. C. van Oosrchot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. https://doi.org/10.1201/9781439821916

[8] G. L. Mullen and D. Panario (Eds.), *Hanbook of Finite Fields*, CRC Press, Boca Raton, FL, 2013.

Received: October 5, 2018; Published: October 23, 2018