SARAJEVO JOURNAL OF MATHEMATICS
Vol.1 (13) (2005), 21–26

REPRESENTATION OF POLYNOMIALS OVER FINITE FIELDS WITH CIRCULANTS

AMELA MURATOVIĆ

Abstract. Representation of polynomials over complex fields is well known. In this paper a similar representation is given for polynomials of degree less than $q-1$, over finite fields. The results are theorems that characterize the centralizer of the circulant of a permutation polynomial, and a formula for the calculation of the determinant of the circulant as the product of the determinants of the polynomials defined on the cosets of some multilpicative subgroup.

1. Introduction

Let p be a prime, n be a positive integer and $q = p^n$. Let F_q be a Galois field of order q. Every mapping $\Psi : F_q \longrightarrow F_q$ can be represented by a unique polynomial $f \in F_q[x]$ of degree less or equal to $q-1$. The induced polynomial is given by formula

$$f(x) = \sum_{c \in F_q} \Psi(c)(1 - (x-c)^{q-1}) \tag{1}$$

or by the Lagrange interpolation formula. We say that polynomial is in normalized form if $a_{q-1} = 0$ and if the polynomial is monic. Note that mapping induced by the polynomial $g(x) = ax + b$ is a bijection. Every polynomial can be reduced to the normalized form by composing it with a suitable linear polynomial. Many properties such as the cardinality of the codomain are preserved with this composition. Here we are interested in the representation of the polynomials, of the degree less or equal to q-2, with circulant matrices. Let polynomial $f(x) = \sum_{i=0}^{q-2} a_i x^i$ be defined on the field F_q. Consider the distinct elements $b_1 = 1, b_2, \ldots, b_{q-1}$ of the field F_q different from zero. Let $V = V(b_1 = 1, b_2, \ldots, b_{q-1})$ be the Vandermonde

2000 *Mathematics Subject Classification.* 12E05, 16S50.

matrix,

$$V = \begin{bmatrix} 1 & 1 & \dots & 1 \\ b_1 & b_2 & \dots & b_{q-1} \\ b_1^2 & b_2^2 & \dots & b_{q-1}^2 \\ \dots & \dots & \dots & \dots \\ b_1^{q-2} & b_2^{q-2} & \dots & b_{q-1}^{q-2} \end{bmatrix}.$$

It is known that V is a regular matrix. Associated with the polynomial f there is the corresponding $(q-1)\times(q-1)$ circulant

$$A = A[a_o, a_1, \dots, a_{q-2}] = \begin{bmatrix} a_0 & a_1 & \dots & a_{q-2} \\ a_{q-2} & a_0 & \dots & a_{q-3} \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots a_{q-2} & a_0 \end{bmatrix}.$$

2. Preliminaries

Note that $(A)_{i,j} = a_{[q-1-i+j] \bmod (q-1)} = a_{(j-i) \bmod (q-1)}$ and $(V)_{i,j} = b_j^{i-1}$. We have

$$\begin{aligned}(AV)_{ij} &= \sum_{k=1}^{q-1}(A)_{i,k}(V)_{k,j} = \sum_{k=1}^{q-1} a_{(k-i) \bmod q-1}\, b_j^{k-1} \\ &= \sum_{k=i}^{q-1} a_{k-i}\, b_j^{(k-i)+(i-1)} + \sum_{k=1}^{i-1} a_{(q-1)+(k-i)}\, b_j^{(q-1+(k-i))+(i-1)} \\ &= \sum_{t=0}^{q-1-i} a_t b_j^{t+(i-1)} + \sum_{t=q-i}^{q-2} a_t b_j^{t+(i-1)} = b_j^{i-1}\sum_{t=0}^{q-2} a_i b_j^t = b_j^{i-1} f(b_j)\end{aligned}$$

for all $i, j \in \{1, 2, \dots, q-1\}$. Thus $AV = V \cdot \mathrm{Diag}\left\{f(b_1), \dots, f(b_{q-2})\right\}$ for all $i, j \in \{1, 2, \dots, q-1\}$. Denote $D_f = \mathrm{Diag}\left\{f(b_1), f(b_2), \dots f(b_{q-1})\right\}$. Then $V^{-1}AV = D_f$. Use of circulant matrices over finite fields is known. Here we mention two results which follow from the last formula:

Theorem of Kenig-Radosh: A polynomial of the degree less than $q-1$ has r nonzero roots if and only if the rank of the corresponding circulant is $q-1-r$ (see [1]).

Rausnitz criterion: A polynomial $f(x)$ is a permutation polynomial if and only if the $\deg(f(x)) < q-1$ and the $\det(A - \lambda I) = \frac{\lambda^q - \lambda}{\lambda - a_0}$, (see [3] and [4]).

Also, in the case of complex fields, the representation by circulants polynomials over the complex roots of the unit element, is well known (see [2]).

3. The main results

Here we want to make a similar representation for finite fields and use this result to make new characterization for permutation polynomials. Consider now the polynomial $f(x)|_{F_q^*}$, where $F_q^* = F_q - \{0\}$. Note that the polynomials $f(x)$ and $g(x)$ induce the same mapping on F_q^* if $f(x) = g(x) \bmod (x^{q-1} - 1)$, and so we can consider polynomials of degree less than $q - 1$.

The set

$$R = \left\{ f(x)|_{F_q^*} | f(x) \in F_q[x], \deg f(x) \leq q - 2 \right\}$$

can be equipped with ordinary addition and multiplication defined as

$$(f * g)(x) = f(x) \cdot g(x) \bmod (x^{q-1} - 1),$$

where $\cdot$ is ordinary multiplication of polynomials. Thus $(R, +, \cdot)$ is a commutative ring with identity. Also $(B, +, \cdot)$, where B is set of diagonal $(q-1) \times (q-1)$ matrices over field F_q, is the a commutative ring with identity. The mapping $f \longrightarrow D_f$, $R \longrightarrow B$, is a homomorphism of rings. Denote

$$C = \left\{ A | A \in M_{q-1 \times q-1}(F_q), \;\; A \text{ is circulant } \right\}.$$

The mapping

$$A \longrightarrow V^{-1} A V = D_f$$

is also a homomorphism of rings. Thus the following theorem holds

Theorem 1.

$$(R, +, \cdot) \simeq (D, +, \cdot) \simeq (C, +, \cdot)$$

and so the corresponding circulants are representations of polynomials over finite fields.

Also we should mention that the Rausnitz criterion implies that the characteristic and minimal polynomials of the circulant corresponding to the permutation polynomial are the same.

The following result gives a new characterization of permutation polynomials over finite fields.

Theorem 2. *Let $f(x) = \sum_{i=0}^{q-2} a_i x^i$ be a polynomial and let A be its corresponding circulant. Then, $f(x)$ is a permutation polynomial if and only if the centralizer $Z(A)$ of A is commutative and in that case $Z(A) = C$.*

Proof. Assume that $f(x)$ is a permutation polynomial. For any B in $Z(A)$, $BA = AB$. Then

$$(V^{-1} A V)(V^{-1} B V) = (V^{-1} B V)(V^{-1} A V) \Rightarrow$$
$$D_f (V^{-1} B V) = (V^{-1} B V) D_f \Rightarrow$$

$$((D_f(V^{-1}BV))_{i,j} = ((V^{-1}BV)D_f)_{i,j} \Rightarrow$$
$$f(b_i)(V^{-1}BV)_{i,j} = (V^{-1}BV)_{i,j}f(b_j).$$

If $i \neq j$, then $f(b_i) \neq f(b_j)$. The equality above implies that $(V^{-1}BV)_{i,j} = 0$. But then $(V^{-1}BV)$ is a diagonal matrix, which implies that B is circulant. Thus $Z(A) \subseteq C$. But since all polynomials commute with f, all circulants commute with A and we have $C \subseteq Z(A)$ and thus $C = Z(A)$ and $Z(A)$ is commutative.

Suppose now that $f(x)$ is not a permutation polynomial. We want to show that $Z(A)$ is not commutative. First assume that $f(b_{i_0}) = f(b_{j_0})$ for some $i_0 \neq j_0$, $b_{i_0}, b_{j_0} \in F_q^*$. Define the matrix $B_1 = (\beta_{i,j})$, where $\beta_{i,j} = 1$ if $i = j$ or, if $i = i_0, j = j_0$, and 0 otherwise.

Then

$$(DB_1)_{i,j} = f(b_i)(B_1)_{i,j} = \begin{cases} f(b_i), & \text{for} \quad i = j, \\ f(b_{i_0}), & \text{for} \quad i = i_0, j = j_0, \\ 0, & \text{otherwise.} \end{cases}$$

Since, $f(b_{i_0}) = f(b_{j_0})$, and $f(b_i) = f(b_j)$, we have $DB_1 = B_1D$. Similarly, the matrix $C_1 = (\gamma_{ij})$ defined by

$$\gamma_{ij} = \begin{cases} 1, & \text{if} \quad i = j, \\ 1, & \text{if} \quad i = j_0, j = i_0, \\ 0, & \text{otherwise,} \end{cases}$$

commutes with D. But

$$(C_1B_1)_{i_0,i_0} = \sum_{k=1}^{q-1}(C_1)_{i_0,k}(B_1)_{k,i_0} = \sum_{k=1}^{q-1}(C_1)_{i_0,k}\delta_{i_0}^k = (C_1)_{i_0,i_0} = 1$$

and

$$(B_1C_1)_{i_0,i_0} = \sum_{k=1}^{q-1}(B_1)_{i_0,k}(C_1)_{k,i_0} = (B_1)_{i_0,i_0} \cdot 1 + (B_1)_{i_0,j_0} \cdot 1 = 2$$

thus $C_1B_1 \neq B_1C_1$. Define $B = V^{-1}B_1V$ and $C = V^{-1}C_1V$. Then $B, C \in Z(A)$ but $BC \neq CB$ so $Z(A)$ is not commutative. Note that for the case when $f(0) = f(b)$ and all other values of f are distinct the degree k, of the polynomial f, satisfies

$$|V_f| \leq q - \left\lceil \frac{q-1}{k} \right\rceil$$

where $\lceil m \rceil$ denotes the smallest integer $\geq m$. Thus,

$$q - 1 \leq q - \left\lceil \frac{q-1}{k} \right\rceil$$

what implies that $k = q - 1$ and this is a contradiction. □

The calculation of determinants of the large order is long, so the following theorem gives a formula for the determinant expressed in terms of determinants of smaller order.

Theorem 3. *Let $f(x) = \sum_{j=0}^{q-2} a_j x^j$ be a polynomial in $F_q[x]$, $q = p^n$. Denote the determinant of the corresponding circulant matrix by $C_{q-1}(f(x))$. Let $k|q-1$. Denote by $S = \{x^{\frac{q-1}{k}} : x \in F^*\}$ the subgroup of the multiplicative group $F_q - \{0\} = F^*$. Let r_j, $j = 1, 2, \ldots, \frac{q-1}{k}$ be representatives of the cosets of S. Consider the polynomials*

$$f_j(x) = \sum_{i=0}^{k-1} \Big(a_i r_j^i + a_{i+k} r_j^{i+k} + a_{i+2k} r_j^{i+2k} + \cdots + a_{i+\lfloor \frac{q-1}{k} \rfloor} r_j^{i+\lfloor \frac{q-1}{k} \rfloor} \Big) x^i$$

and denote the determinant of the corresponding $k \times k$ circulant by $C_k(f_j(x))$, for $j = 1, 2, \ldots, \frac{q-1}{k}$. Then

$$C_{q-1}(f_j(x)) = \prod_{j=1}^{\frac{q-1}{k}} C_k(f_j(x)).$$

Proof. Let $r_j S$ be a fixed coset of S in F_q^*. For all elements in $b_l \in r_j S$, $l = 1, 2, \ldots, k$ there is unique $s_l \in S$ such that $b_l = r_j s_l$. Then for fixed l,

$$\begin{aligned} f(b_l) &= \sum_{i=0}^{k-1} a_i b_l^i = \sum_{i=0}^{q-2} a_i r_j^i s_l^i \\ &= \sum_{i=0}^{k-1} \Big(a_i r_j^i + a_{i+k} r_j^{i+k} + a_{i+2k} r_j^{i+2k} + \cdots + a_{i+\lfloor \frac{q-1}{k} \rfloor} r_j^{i+\lfloor \frac{q-1}{k} \rfloor} \Big) s_l^i \\ &= \sum_{i=0}^{k-1} a_i^j s_l^i = f_j(s_l). \end{aligned}$$

Let $s_1, s_2, \ldots, s_k$ be all distinct elements in S, and $V = V(s_1, s_2, \ldots, s_k)$ be the Vandermonde matrix. Let A^j be the circulant $k \times k$ matrix of the polynomial $f_j(s_l)$. Then $(A)_{i,j}^j = a'_{[k-i+j] \bmod k} = a_{(j-i) \bmod k}$ and $(V)_{i,j} = s_j^{i-1}$. We have

$$\begin{aligned} (AV)_{i,j} &= \sum_{t=1}^{k} (A^j)_{i,t} (V)_{t,j} = \sum_{t=1}^{k} a^j_{(t-i) \bmod k} \, s_j^{t-1} \\ &= \sum_{t=i}^{k} a^j_{t-i} \, b_j^{(t-i)+(i-1)} + \sum_{t=1}^{i-1} a^j_{k+(t-i)} \, s_j^{(k+(t-i))+(i-1)} \end{aligned}$$

$$= \sum_{t=0}^{k-i} a_t^j \, s_j^{t+(i-1)} + \sum_{t=k+1-i}^{k-1} a_t^j \, s_j^{t+(i-1)}$$
$$= s_j^{i-1} \sum_{t=0}^{k-1} a_i^j \, s_j^t = s_j^{i-1} f_j(s_j)$$

for all $i, j \in \{1, 2, \ldots, k\}$. Thus similarly as before

$$V^{-1} A^j V = \text{Diag}\left\{f_j(s_1), f_j(s_2), \ldots, f_j(s_k)\right\} = \text{Diag}\left\{f(b_1), f(b_2), \ldots, f(b_k)\right\}.$$

Thus

$$\det(A^j) = C_k(f_j(x)) = \prod_{b \in r_j S} f(b) = \prod_{s \in S} f_j(s).$$

Finally

$$C_{q-1}(f(x)) = \prod_{s \in F_q^*} f(s) = \prod_{j=1}^{\frac{q-1}{k}} \Big(\prod_{b \in r_j S} f(b) \Big) = \prod_{j=1}^{\frac{q-1}{k}} C_k(f_j(x)).$$

□

References

[1] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, V. 20, Cambrige University Press, 1984.

[2] P. J. Davis, *Circulant Matrices*, John Wiley and Sons, 1979.

[3] R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field*, Amer. Math. Monthly, 95 (1988), 233–236.

[4] R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field II*, Amer. Math. Monthly, 95 (1993), 71–74.

(Received: October 26, 2004)
(Revised: November 22, 2004)

University of Sarajevo
Faculty of Science
Department of Mathematics
Zmaja od Bosne 33–35
71000 Sarajevo
Bosnia and Herzegovina
E–mail : amela@pmf.unsa.ba