A NOTE ON
POLYNOMIAL MATRIX FUNCTIONS
OVER A FINITE FIELD

BY

J. V. BRAWLEY*

DEPARTMENT OF MATHEMATICAL SCIENCES
Clemson University

TECHNICAL REPORT #256
Contract Report N8

*Research supported by
The Offices of Naval Research
Contract N00014-76-C-0130

REPRODUCTION IN WHOLE OR PART IS PERMITTED FOR ANY PURPOSES OF
THE U.S. GOVERNMENT. DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED.
A Note on Polynomial Matrix Functions
over a Finite Field
by J.V. Brawley*

1. Let \( F = GF(q) \) denote the finite field of order \( q \), and let \( F_n \) denote the ring of \( nxn \) matrices over \( F \). Consider an element \( A(x) \in F_n[x] \); i.e.,

\[
A(x) = A_NN^N + A_{N-1}N^{N-1} + \ldots + A_1x + A_0
\]

where \( A_i \in F_n \). This polynomial defines via substitution several functions from \( F_{n} \) to \( F_{n} \). Two such functions are

\[
B \rightarrow A_r(B) = A_NB^N + A_{N-1}B^{N-1} + \ldots + A_1B + A_0
\]

and

\[
B \rightarrow A_L(B) = B^NA_N + B^{N-1}A_{N-1} + \ldots + BA_1 + A_0
\]

We call (2) and (3), respectively, the right and left polynomial functions determined by \( A(x) \) with the terms right and left indicating the side on which the substituting variable is placed.

*Supported in part by ONR contract N00014-76-C-0130.
Definition. A function $A: F_n \to F_n$ is called a right (respectively left) polynomial function if there exists a polynomial $A(x) \in F_n[x]$ which represents $A$ via the right substitution (2) (respectively (3)).

In this note we obtain unique representations for and determine the number of right (left) polynomial functions $A: F_n \to F_n$. Proofs will be given for the right functions which can be obviously modified for the left polynomial functions.

2. Recall that

$$L_n(x) = \prod_{i=1}^{n} (x^{q^i} - x)$$

is the monic polynomial of least degree in $F[x]$ satisfied by every $B \in F_n$; indeed, $L_n(x)$ is the least common multiple of all degree $n$ polynomials in $F[x]$ [See, 2]. We define $\delta$ by

$$\delta = \deg L_n(x) = q^n + q^{n-1} + \ldots + q.$$

**Theorem 1.** Let $Z(x) = \sum_{i=0}^{N} Z_i x^i$ be a polynomial in $F_n[x]$ with $\deg Z(x) = N < \delta$. If $Z(r)(B) = Z_NB^N + \ldots + Z_1B + Z_0 = 0$ for every $B \in F_n$, then $Z_i = 0$, $i = 0, 1, 2, \ldots, N$.

**Proof.** Let $f(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_1x - a_0$ be an arbitrary polynomial of degree $n$ in $F[x]$, and let $C \in F_n$ denote the companion matrix of $f(x)$. Dividing $Z(x)$ by $f(x)$ we obtain

$$Z(x) = Q(x) f(x) + R(x)$$
where \( Q(x) \) and \( R(x) \) are in \( F_n[x] \) with

\[
R(x) = R_{n-1}x^{n-1} + \ldots + R_1x + R_0.
\]

Since \( f(x) \) is a scalar polynomial we may substitute an arbitrary matrix \( B \) into (6) to get

\[
Z_r(B) = Q_r(B)f(B) + R_r(B).
\]

In particular, for every nonsingular \( P \in GL(n,q) \) it follows from the Hamilton-Cayley theorem that

\[
0 = Z_r(PCP^{-1}) = R_r(PCP^{-1}).
\]

Thus \( (R_r(PCP^{-1}))P = 0 \) or

\[
R_{n-1}PC^{n-1} + R_{n-2}PC^{n-1} + \ldots + R_1PC + R_0P = 0
\]

for every \( P \in GL(n,q) \).

Now it is known [1] that each matrix \( X \in F_n \) can be written as a linear combination of nonsingular matrices \( P_i \); i.e.,

\[
X = c_1P_1 + c_2P_2 + \ldots + c_tP_t, c_i \in F.
\]

If follows from (8) that

\[
R_{n-1}XC^{n-1} + R_{n-2}XC^{n-1} + \ldots + R_1XC + R_0X = 0
\]

for every \( X \in F_n \). In particular, if we take \( X = E_m \) where \( E_m \)
has a 1 in position \((m,1)\) and zeros elsewhere we find through actual computation that equation (9) reduces to
$$\begin{pmatrix}
  r_{1m}^{(0)} & r_{1m}^{(1)} & \ldots & r_{1m}^{(n-1)} \\
  r_{2m}^{(0)} & r_{2m}^{(1)} & \ldots & r_{2m}^{(n-1)} \\
  \vdots & \vdots & \ddots & \vdots \\
  r_{nm}^{(0)} & r_{nm}^{(1)} & \ldots & r_{nm}^{(n-1)}
\end{pmatrix} = 0$$

where $R_k = (r_{ij})$. Thus column $m$ of $R_k$ is zero for $k = 0, 1, \ldots, n-1$ and $m = 1, 2, \ldots, n$; i.e., $R_k = 0$ for $k = 0, 1, \ldots, n-1$. It follows from (6) that $f(x)$ divides $Z(x)$ for every monic of degree $n$; hence $L_n(x)$ divides $Z(x)$. But $\deg Z(x) < \deg L_n(x)$ so $Z(x)$ must be the zero polynomial; i.e., every $Z_i = 0$ and the proof is complete.

As a corollary to Theorem 1, we have the following:

**Theorem 2.** Each right polynomial function $A: F_n \rightarrow F_n$ can be represented uniquely by a polynomial $A(x) \in F_n[x]$ of degree $< \delta$ and each such polynomial represents a right polynomial function. The number of right polynomial functions is therefore $q^{n^2\delta}$.

**Proof.** If $A_1(x)$ and $A_2(x)$ have degree $< \delta$ and each represent the right polynomial function $A$ then $A_1(x) - A_2(x)$ represents the zero function; hence by Theorem 1, $A_1(x) = A_2(x)$.

Finally let $A$ be a right polynomial function and let $A(x)$
represent A. By division

\[ A(x) = Q(x)L_n(x) + R(x) \]

where \( R(x) \) has degree \( < \delta \). Clearly, \( R(x) \) represents A.

References


Let $F = GF(q)$ denote the finite field of order $q$, and let $F_n^m$ denote the ring of $n \times n$ matrices over $F$. Each matrix polynomial $A(x) = A_N x^N + \ldots + A_1 x + A_0$ in $F_n[x]$ defines via substitution several functions from $F_n^m$ to $F_n^m$. Two such functions, called respectively, the right and left polynomial functions determined by $A(x)$ are

$$B \to A_R(B) = A_N B^N + \ldots + A_1 B + A_0$$
$$B \to A_L(B) = B^N A_N + \ldots + B A_1 + A_0$$

A function $A: F_n^m \to F_n^m$ is called a right (left) polynomial function if there exists $A(x) \in F_n[x]$ which represents $A$ via the right (left) substitution $B \to A_R(B)$ ($B \to A_L(B)$). This paper obtains a unique representation for and determines the number of right (left) polynomial functions $A: F_n^m \to F_n^m$. 