Matrix Representations of $GF(p^n)$ over $GF(p)$

Peter M. Maurer
Dept. of Computer Science
Baylor University
Waco, Texas 76798

Abstract – We show that any non-singular $n \times n$ matrix of order $p^n - 1$ over $GF(p)$ is a generator of a matrix representation of $GF(p^n)$. We also determine the number of matrix representations of $GF(p^n)\, GF(p)$ over $GF(p)$, and then number of order $p^n - 1$ matrices in the general linear group of degree n over $GF(p)$. The theorems are easily generalizable to arbitrary field extensions.

1. Text

The following contains some results about the matrix representations of $GF(p^n)$ over $GF(p)$. I'm not claiming to be the first to write this stuff down, but I'm the first I know of, and the proofs are all mine.

Theorem 1. Let M be a non-singular $n \times n$ matrix over $\mathrm{GF}(p)$, which is of order $p^n - 1$. Let $K = \left\{Z, M^0, M^1, M^2, \ldots, M^{p^n-1}\right\}$, where Z is the $n \times n$ zero-matrix. Then K is isomorphic to $\mathrm{GF}(p^n)$ under matrix addition and multiplication.

Proof: Let P be the characteristic polynomial of M. P must have one root of order $p^n - 1$, namely, M, itself. P must be irreducible, for if it were not, each root, α, of P must occur in some finite field of order p^k, with $k < n$. However, since the multiplicative group of $GF(2^k)$ is of size $p^k - 1 < p^n - 1$, α cannot be of order $p^n - 1$. Therefore P is irreducible and its roots must generate $GF(p^n)$. Since P has a root of order $p^n - 1$ it is also primitive. Thus any root of P which is of order $p^n - 1$, including M, must be a generator of the multiplicative group of $GF(p^n)$. ■

Corollary: Let M be a non-singular $n \times n$ matrix over $\mathrm{GF}(p)$, which is of order $p^n - 1$. Then the characteristic polynomial of M is irreducible and primitive.

Theorem 2. Given a polynomial $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ of degree n over $GF(p)$, with $a_0 \neq 0$. Let M be the matrix:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Then M is of order $p^n - 1$ if and only if P is primitive.

Proof. A quick calculation will show that that P is the characteristic polynomial of M. By the corollary to Theorem 1, if M is of order $p^n - 1$ then P is primitive. If P is primitive, it must have a root of order $p^n - 1$. Since P is of degree n it must split in $GF(p^n)$. Let M' $GF(p^n)$ be the diagonal matrix over $GF(p^n)$ of the following form:

$$M' = \begin{pmatrix} e_1 & 0 & \ldots & 0 \\ 0 & e_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e_n \end{pmatrix}$$

Where e_i is the i^{th} root of P. The e_i are the eigenvalues of M, so M and M' are similar and must be of the same order. Since P has at least one root of order $p^n - 1$ there must be an element e_j order $p^n - 1$. Now,

$$M'^k = \begin{pmatrix} e_1^k & 0 & \ldots & 0 \\ 0 & e_2^k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e_n^k \end{pmatrix}$$

Because e_j is of order $p^n - 1$, for all k, $1 < k < p^n - 1$ $e_j^k \neq 1$, and $M'^k \neq I$. But because the order of the multiplicative group of $GF(p^n)$ is $p^n - 1$, the order of every element of $GF(p^n)$ must divide $p^n - 1$, so $e_i^{2^p - 1} = 1$ for all i, $1 \leq i \leq n$, and $M'^{p^n - 1} = I$. Thus the order of M' is equal to $p^n - 1$ and the order of M is $p^n - 1$ as well. ■

Theorem 2 gives us a way to test for primitive polynomials. Given P, we formulate M, and determine the order of M. If the result is $p^n - 1$, then p is primitive.

We can also say something about the structure of $G=\left\{M, M^2,...,M^{p^n-1}\right\}$. The number of order p^n-1 matrices in G is $\phi\left(p^n-1\right)$. Each of these matrices as a characteristic polynomial P of degree n which is irreducible and primitive. Each such polynomial has exactly n distinct roots in G. There are $\frac{\phi\left(p^n-1\right)}{n}$ primitive polynomials of degree n over $GF\left(p\right)$. Therefore, we have the following theorem.

Theorem 3. Let M be an $n\times n$ matrix of order p^n-1 over $GF\left(p\right)$ and let $G=\left\{M, M^2,...,M^{p^n-1}\right\}$. For every primitive polynomial P of degree n over $GF\left(p\right)$, G contains exactly n matrices with characteristic polynomial P.

How many conjugates are there of the multiplicative group $G=\left\{M, M^2,...,M^{p^n-1}\right\}$? We need to determine the normalizer of G in $GL_n\left(p\right)$, that is we need to determine all matrices $N\in GL_n\left(p\right)$ such that $N^{-1}M^iN\in G$ for all i, $1\le i\le p^{n-1}$. Since $N^{-1}M^iNN^{-1}M^jN=N^{-1}M^iIM^jN=N^{-1}M^iM^jN$, the transformation $T_N\left(M^i\right)=N^{-1}M^iN$ is an automorphism of G. T_N is one-to-one is because T_N is order preserving making the kernel of T_N equal to $\left\{I\right\}$. Because $T_N\left(0\right)=N^{-1}0N=0$, and $N^{-1}M^iN+N^{-1}M^jN=N^{-1}\left(M^iN+M^jN\right)=N^{-1}\left(M^i+M^j\right)N$, T_N is also an automorphism of $GF\left(p^n\right)$. Furthermore, T_N preserves $GF\left(p\right)$. In any matrix representation of $GF\left(p^n\right)$, 1 must be represented as the identity matrix I, any element k of $GF\left(p\right)$ must be represented as the matrix kI, where $2I=I+I$ and $kI=(k-1)I+I$. Thus k is represented by a matrix with k's along the main diagonal, and zeros elsewhere. We will write these matrices as k. Diagonal matrices of this form commute with every matrix, therefore $T_N(k)=T^{-1}kT=T^{-1}Tk=k$.

The distinct automorphisms of $GF\left(p^n\right)$ are generated by the conjugates of M: M^p, M^{p^2}, …, $M^{p^{n-1}}, M^{p^n}=M$. Every element has n conjugates in $GF\left(p^n\right)$. For each power of p, we define the transformation $Q_{p^i}(a)=a^{p^i}$. The transformations Q_{p^i} are the distinct automorphisms of $GF\left(p^n\right)$ that preserve $GF(p)$.

Let N be a matrix such that $Q_{p^i}=T_N$. (We still need to prove this exists.) For any matrix $M^i\in G$, $T_{M^kN}=Q_{p^i}$ because $\left(M^kN\right)^{-1}=N^{-1}\left(M^k\right)^{-1}$ and $T_{M^kN}\left(M^i\right)=N^{-1}\left(M^k\right)^{-1}M^iM^kN=N^{-1}\left(M^k\right)^{-1}M^kM^iN=N^{-1}M^iN=T_N\left(M^i\right)$. Therefore, the number of matrices in the normalizer of G is $o(G)n = np^n - n$. Therefore the number of representations of $GF(p^n)$ in $n \times n$ matrices is $\dfrac{\prod_{i=0}^{n-1}(p^n - p^i)}{np^n - n}$.

Theorem 4. If M is a non-singular matrix $n \times n$ of order p^{n-1} over $GF(p)$, then there is a matrix N over $GF(p)$ such that $N^{-1}MN = M^p$.

Proof. Let P be the characteristic polynomial of M. The matrix M must be similar to the following matrix over $GF(p)$,

$$M' = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_k \end{pmatrix}$$

Where the C_i are the companion matrices of the irreducible factors of P. However, by Theorem 1, we know that P must be irreducible, therefore

$$M' = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Where the a_i are the coefficients of P. If a is any root of P, then a must be primitive, and the set $\left\{a, a^p, a^{p^2}, \ldots, a^{p^{n-1}}\right\}$ is the complete set of roots of P. This implies that M is similar, in $GF(p^n)$ to the matrix

$$M'' = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a^p & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{p^{n-1}} \end{pmatrix}$$

In general, if two matrices A and B are similar, then $A = N^{-1}BN$ for some non-singular matrix N. Now, we have $A^2 = N^{-1}BBN = N^{-1}B^2N$, so in general we will have A^k similar to B^k. In particular, M^p is similar to

$$M''^{p} = \begin{pmatrix} a^{p} & 0 & \dots & 0 \\ 0 & a^{p+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^{p^n} \end{pmatrix}$$

But $a^{p^n} = a$ so M''^{p} and M' have the same eigenvalues and the same characteristic polynomial. Thus, M and M^p have the same characteristic polynomial, P. Since M^p has characteristic polynomial P, it must be similar to M'. Since M and M^p are both similar to M' in $GF(p)$, they must be similar to one another in $GF(p)$.■

Definition. We will call a non-singular $n \times n$ matrix, M, over $GF(p)$ *primitive*, if it is of order $p^n - 1$.

Theorem. Let R_1 and R_2 be two $n \times n$ matrix representations of $GF(p^n)$ over $GF(p)$. If $M \in R_1 \cap R_2$ and M is primitive, then $R_1 = R_2$.

Proof. If R_1 is a matrix representation of $GF(p^n)$ and $M \in R_1$ is primitive, then $R_1 = \{0, M, M^2, M^{p^n-1} = I\}$. Because $M \in R_2$, $R_2 = \{0, M, M^2, M^{p^n-1} = I\} = R_1$.■

Corollary. Any nonsingular $n \times n$ matrix M of order $p^n - 1$ over $GF(p)$ appears in one and only one representation of $GF(p^n)$.

The following two theorems are obvious from the preceding results.

Theorem. Let R be a matrix representation of $GF(p^n)$ over $GF(p)$. Then R contains $\phi(p^n - 1)$ matrices of order $p^n - 1$.

Theorem. $GL_n(p)$ contains $\dfrac{\prod_{i=0}^{n-1}(p^n - p^i)}{np^n - n}\phi(p^n - 1)$ matrices of order $p^n - 1$.