Some Matrix Equations over a Finite Field.

By John H. Hodges (*) (Buffalo, U. S. A.).

Summary. - Explicit formulas are found for the number of solutions over a finite field of several matrix equations, for example: $X'A + A'X = B$. Conditions for solvability are also given.

1. Introduction. - Let $GF(q)$ denote the finite field of $q = p^n$ elements, $p$ odd. In this paper we consider several problems of the following type. If $B$ is a symmetric matrix of order $t$ and $A$ is an arbitrary $m \times t$ matrix, both with elements in $GF(q)$, determine the number of $m \times t$ matrices $X$ over $GF(q)$ such that $X'A + A'X = B$, where the prime denotes transpose. In § 3 it is shown (Theorem 1) that if this equation has any solutions, their number is $q^e$, where $e = t(m - r) + r(r - 1)/2$ and $r$ is the rank of $A$. The theorem also gives a necessary and sufficient condition that the equation have solutions. Explicit solutions (Theorem 2) are given when $m = t = r$.

2. Notation and preliminaries. - Let $GF(q)$, $q = p^n$ odd, denote the finite field of $q$ elements. Lower case Greek letters $\alpha, \beta, ...$ will denote elements of $GF(q)$ except as indicated. Italic capitals $A, B, ...$ will denote matrices over $GF(q)$, except as indicated. $A(m, t)$ denotes a matrix of $m$ rows and $t$ columns and $A(m, t; r)$ a matrix of the same dimensions having rank $r$.

If $A = (x_{ij})$ is square, then $\sigma(A) = \sum x_{ii}$ is the trace of $A$. Clearly, $\sigma(A') = \sigma(A)$, $\sigma(A + B) = \sigma(A) + \sigma(B)$ and $\sigma(AB) = (BA)$.

If $A = A(m, t; r)$, by [1; p. 281, Corollary 1] there exist non-singular $P = P(m, m)$, $Q = Q(t, t)$ such that $PAQ = I(m, t; r)$, where $I(m, t; r)$ is the matrix of $m$ rows and $t$ columns having the identity matrix of order $r$ in its upper left-hand corner and zeros elsewhere.

For $\alpha \in GF(q)$ we define

\begin{equation}
\sigma(\alpha) = e^{2\pi i \sigma(\alpha)}/p, \\
\ell(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}},
\end{equation}

from which it follows that $\sigma(\alpha + \beta) = \sigma(\alpha, e(\beta))$ and

\begin{equation}
\sum_{\alpha} \sigma(\alpha \beta) = \begin{cases} q & (\alpha = 0) \\
0 & (\alpha \neq 0)
\end{cases}
\end{equation}

where the sum is over all $\beta \in GF(q)$.

(*) The research for this paper was supported by National Science Foundation Research Grant G-2900.
3. The equation $X'A + A'X = B$. Let $B$ be symmetric of order $t$ and $A = A(m, t; r)$ be arbitrary. Let $N(A, B)$ denote the number of matrices $X = X(m, t)$ such that

$$X'A + A'X = B. \tag{3.1}$$

Let $P(m, m)$ and $Q(t, t)$ be non-singular such that $PAQ = I(m, t; r)$. Then with $X = P'Y Q^{-1}$, (3.1) reduces to

$$Y'I(m, t; r) + I(t, m; r)Y = QBQ. \tag{3.2}$$

Now, using (2.2) we can show that if $B$ is symmetric of order $t$, then

$$\sum_{C=C} e |(Y'I(m, t; r) + I(t, m; r)Y)C| = 2q^{t(t+1)} \quad (B = 0)$$

$$0 \quad (B \neq 0), \tag{3.3}$$

where the summation is over all symmetric $C$ of order $t$. In view of (3.3) and the relation between (3.1) and (3.2) we have

$$q^{t(t+1)} N(A, B) = \sum_{Y(m, t)} \sum_{C=C} e |(Y'I(m, t; r) + I(t, m; r)Y - QBQC)|$$

$$= \sum_{C=C} e |-(QBQC)| \sum_{Y'(t, m)} e |(2Y'I(m, t; r)C)|, \tag{3.4}$$

where the summations are over all symmetric $C$ of order $t$ and all $Y' = Y'(t, m)$. To evaluate the inner summation in (3.4) we let $Y' = (\xi_{ij}), C = (\gamma_{ij})$ and $I(m, t; r) = (\alpha_{ij})$ where $\alpha_{ij} = 1$ if $1 \leq i = j \leq r$ and 0 otherwise. Then

$$e |(2Y'I(m, t; r)C)| = \prod_{i=1}^{t} \prod_{j=1}^{r} e(2\xi_{ij}\gamma_{ij}), \tag{3.5}$$

so that using the properties of $e(x)$ given in § 2 we have

$$\prod_{i=1}^{t} \prod_{j=1}^{r} e(2\xi_{ij}\gamma_{ij}). \tag{3.6}$$

Then summing (3.5) over all $Y' = Y'(t, m)$ gives

$$\sum_{Y'(t, m)} e |(2Y'I(m, t; r)C)| = q^{t(m-r)} \prod_{i=1}^{t} \prod_{j=1}^{r} e(2\gamma_{ij}\xi_{ij}) \tag{3.7}.$$