RANKED SOLUTIONS OF THE MATRIC EQUATION $A_1 X_1 = A_2 X_2$

A. Duane Porter

Mathematics Department
University of Wyoming
Laramie, Wyoming 82070

Nick Mousouris

Mathematics Department
Humboldt State University
Arcata, California 95521

(Received December 8, 1977 and in Revised form February 20, 1979)

ABSTRACT. Let $GF(p^z)$ denote the finite field of p^z elements. Let A_1 be $s \times m$ of rank r_1 and A_2 be $s \times n$ of rank r_2 with elements from $GF(p^z)$. In this paper, formulas are given for finding the number of X_1, X_2 over $GF(p^z)$ which satisfy the matric equation $A_1 X_1 = A_2 X_2$, where X_1 is $m \times t$ of rank k_1 , and X_2 is $n \times t$ of rank k_2 . These results are then used to find the number of solutions $X_1, \dots, X_n, Y_1, \dots, Y_m, m, n > 1$, of the matric equation $A_1 X_1 \dots X_n = A_2 Y_1 \dots Y_m$.

KEY WORDS AND PHRASES. Finite Field, Matric equation, Ranked Solutions.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES: 15A 24.

1. INTRODUCTION. Let $GF(q)$ denote the finite field with $q = p^z$ elements, p odd. Matrices with elements from $GF(q)$ will be denoted by Roman capitals $A, B, \dots$. $A(n,s)$ will denote a matrix of n rows and s columns, and $A(n,s;r)$ will denote a matrix of the same dimensions with rank r . I_r denotes the identity matrix of order r , and $I(n,s;r)$ denotes a matrix of n rows and s columns having I_r in its upper left hand corner and zeros elsewhere.

In this paper we find the number of solutions $X_1(m,t;k_1), X_2(n,t;k_2)$ to the matrix equation

$$A_1 X_1 = A_2 X_2, \quad (1.1)$$

where $A_1 = A_1(s,m;r_1)$ and $A_2 = A_2(s,n;r_2)$. Since the ranks of X_1, X_2 are specified, we call this the ranked case. If the ranks were not specified, we would call it the unranked case. In section 4 we apply this result to find the number of solutions $X_1, \dots, X_n, Y_1, \dots, Y_m$, $m, n \geq 1$, to the matrix equation

$$A_1 X_1 \dots X_n = A_2 Y_1 \dots Y_m, \quad (1.2)$$

both in the unranked and ranked cases.

Equation (1.1) is a special case of the matrix equation

$$A_1 X_1 + \dots + A_n X_n = B, \quad (1.3)$$

and equation (1.2) is a special case of the more general equation

$$A_1 X_{11} \dots X_{1m(1)} + \dots + A_n X_{n1} \dots X_{nm(n)} = B. \quad (1.4)$$

Porter [6] found the number of solutions $X_1, \dots, X_n$ to (1.3) in the unranked case. We could find the number of solutions to (1.3) in the ranked case if we could find the number of ranked solutions to $A_1 X_1 + A_2 X_2 = B$. The number of ranked solutions to $A_1 X_1 + A_2 X_2 = B$ together with the formulae for the number of solutions to $X_1 \dots X_n = B$ would give the number of solutions to (1.4). The number of unranked solutions to $X_1 \dots X_n = B$ is given by Porter in [5]. The

number of ranked solutions to $X_1 \dots X_n = B$ appears in [9], by the authors.

Presently the authors know of no published results, unranked or ranked, giving the number of solutions to (1.4) except when (1.4) reduces to (1.3). There are partial results in the unranked case to the analogous problem

$U_a \dots U_1 A + B V_1 \dots V_b = C$. Hodges [1] found the number of unranked solutions with $a = b = 1$. Hodges [2] and Porter [7] found partial results in the unranked case when a, b are arbitrary and Hodges [3] discussed ranked solutions when $a = b = 1$.

2. NOTATION AND PRELIMINARIES. A well known formula due to Landsberg [4] gives the number $g(m, t; s)$ of $m \times t$ matrices of rank s over $GF(q)$.

$$g(m, t; s) = q^{s(s-1)/2} \prod_{i=1}^s (q^{m-i+1} - 1)(q^{t-i+1} - 1)/(q^i - 1), \quad (2.1)$$

for $1 \leq s \leq \min(m, t)$, $g(m, t; 0) = 1$, and $g(m, t; s) = 0$ for $\min(m, t) < s$ or $s < 0$.

If $X = X(e, t)$ and $X = \text{col}[U, Y]$, where U is fixed, $U = U(m, t; s)$ and $Y = Y(e - m, t)$, then the number of ways that Y can be chosen such that X has rank k is given by Porter and Riveland [11] to be

$$G(e, t, m; k, s) = q^{s(e-m)} g(e - m, t - s; k - s). \quad (2.2)$$

In [9, Theorem 3] the authors found the number of solutions $X(m, f; k)$ to the matrix equation $AX = B$, where $A = A(s, m; \rho)$ and $B = B(s, f; \beta)$. This number is given by

$$N(A, B, k) = h(B_0) q^{(m-\rho)\beta} g(m - \rho, f - \beta; k - \beta) = h(B_0) L(m, f; \rho, \beta, k), \quad (2.3)$$

where $h(B_0)$ is defined as follows. If P, Q are nonsingular matrices such that $PAQ = I(s, m; \rho)$, then $B_0 = PB = (\beta_{ij})$ and $h(B_0) = 1$ if $\beta_{ij} = 0$ for $i > \rho$, $h(B_0) = 0$ otherwise. The number of solutions, when there are any, is denoted by $L(m, f; \rho, \beta, k)$.

Let $A = A(n, s; r)$ and $B = B(n, t; u)$. Then Porter [5] showed that the number

of solution $X_1(s, s_1), X_i(s_{i-1}, s_i)$ for $1 < i < a$, $X_a(s_{a-1}, t)$ to the matrix equation $AX_1 \dots X_a = B$. when there are solutions, is given by

$$N(a, s, t, s_1, r, u) = q^{t(s_{a-1}-r) + ss_1 + s_1s_2 + \dots + s_{a-2}s_{a-1}} \sum_{z_{a-1}=0}^{\min(r, t)} H(r, t, y; z_{a-1}). \quad (2.4)$$

$$\cdot q^{-z_{a-1}s_{a-1}} \prod_{i=2}^{a-1} \sum_{z_{a-1}=0}^{\min(z_{a-i+1}, s_{a-i+1})} g(z_{a-i+1}, s_{a-i+1}; z_{a-i}) q^{-z_{a-i}s_{a-i}},$$

where $g(m, t; s)$ is given by (2.1), and $H(s, t, u; z)$ is given in [1] to be

$$H(s, t, u, z) = q^{uz} \sum_{j=0}^z (-1)^j q^{j(j-2u-1)/2} \begin{bmatrix} u \\ j \end{bmatrix} g(s-u, t-u; z-j),$$

where the bracket denotes the q -binomial coefficient defined for non-negative integers by

$$\begin{bmatrix} u \\ 0 \end{bmatrix} = 1, \begin{bmatrix} u \\ j \end{bmatrix} = \prod_{i=0}^{j-1} (1 - q^{u-1}) / (1 - q^{i+1}) \quad \text{if } 1 \leq i \leq u, \begin{bmatrix} w \\ j \end{bmatrix} = 0$$

if $j > w$. For the purposes of this paper we take $A = I_s$ in (2.4). By [5] there will always be solutions to $X_1 \dots X_a = B$, and this number can be represented by

$$M_a(s, s_1, \dots, s_{a-1}, t, u) = \begin{cases} N(a, s, t, s_1, s, u) & \text{for } a \geq 2, \\ 1 & \text{for } a = 1. \end{cases} \quad (2.5)$$

The number of matrices $D = D(a, b; c)$ such that $D = \text{col}[D_1, D_2]$ where $D_1 = D_1(d, b)$ and $D_2 = D_2(a-d, b; c-d)$, $d \leq \min(a, c)$ is given in [10] to be $K(a, b, c, d) = q^{(c-d)d} g(d, b+d-c; d) g(a-d, b; c-d)$. The number $T_n(d_0, \dots, d_n; k_1, \dots, k_n, \beta)$ of solutions $X_1(d_0, d_1; k_1), \dots, X_n(d_{n-1}, d_n; k_n)$ to the matrix equation $X_1 \dots X_n = B$, where $B = B(d_0, d_n; \beta)$, is given in [9] by the

following three formulae:

$$\begin{aligned}
 T_1(d_0, d_1; k_1, \beta) &= \begin{cases} 0 & \text{if } k_1 \neq \beta, \\ 1 & \text{if } k_1 = \beta, \end{cases} \\
 T_2(d_0, d_1, d_2; k_1, k_2, \beta) &= K(d_0, d_1, k_1, \beta) L(d_1, d_2; k_1, \beta, k_2), \quad (2.6) \\
 T_n(d_0, \dots, d_n; k_1, \dots, k_n, \beta) &= \sum_{i_n=\beta}^{r_n} \sum_{i_{n-1}=i_n}^{r_{n-1}} \dots \sum_{i_3=i_4}^{r_3} T_2(d_0, d_{i_1}, k_1, k_2, i_3) \cdot \\
 &\quad \cdot \prod_{m=3}^n K(d_0, d_{m-1}, i_m, i_{m+1}) L(d_{m-1}, d_m, i_m, i_{m+1}, k_m),
 \end{aligned}$$

where $n \geq 3$, $r_j = \min(k_1, \dots, k_{j-1})$ for $j = 3, \dots, n$ and $i_{n+1} = \beta$.

3. THE MAIN RESULT.

THEOREM 1. If $A = A(s, m; \rho)$, then the number of solutions $X_1(m, t; k_1)$.

$X_2(s, t; k_2)$, for $\rho, k_1 \geq k_2$, to the matrix equation

$$AX_1 = X_2, \quad (3.1)$$

is given by $N(m, t; \rho, k_1, k_2) = g(\rho, t; k_2) L(m, t; \rho, k_2, k_1)$, where $g(\rho, t; k_2)$ is evaluated using (2.1) and $L(m, t; \rho, k_2, k_1)$ is evaluated using (2.3).

PROOF: Let P, Q be nonsingular matrices such that $PAQ = I(s, m; \rho)$. Then (3.1) can be rewritten as

$$I(s, m; \rho) Q^{-1} X_1 = P X_2. \quad (3.2)$$

The left hand side of (3.2) is of the form $\text{col}[Y, 0]$ where $Y = Y(\rho, t)$. For a particular $X_2(s, t; k_2)$, there will be matrices $X_1(m, t; k_1)$ which satisfy (3.2), and therefore (3.1), provided X_2 is the product of P^{-1} and a matrix of the form $\text{col}[Y, 0]$ where $Y = Y(\rho, t; k_2)$. Since P^{-1} is nonsingular there are the same number of matrices X_2 with this property as there are $\rho \times t$ matrices of rank k_2 . The number of $\rho \times t$ matrices of rank k_2 is given by Landsberg's formula (2.1) and denoted by $g(\rho, t; k_2)$. For each such X_2 the number of X_1 such that X_1, X_2 satisfy (3.1) can be represented by $L(m, t; \rho, k_2, k_1)$ as given by (2.3). Therefore the number of solutions X_1, X_2 to (3.1) is given by $g(\rho, t; k_2)L(m, t; \rho, k_2, k_1)$, and the theorem is proved.

It should be noted that Theorem 1 is a special case of a theorem of Hodges [3]. However, our proof, and so the form of the resulting formula, is quite different since Hodges uses exponential sums in his proof and we do not. Our proof of Theorem 1 is consistent with the methods of proof used in the rest of this paper.

THEOREM 2. Let $A = A(s, m; \rho) = \text{col}[A_1, A_2]$ where $A_1 = A_1(n, m; \alpha_1)$ and $A_2 = A_2(s - n, m; \alpha_2)$ with $n \leq s$. Let P, Q be nonsingular matrices such that $PA_2Q = I(s - n, m; \alpha_2)$ and $A_1Q = [B_1, B_2]$ where $B_2 = B_2(n, m - \alpha_2; \beta)$. Then the number of solutions $X_1(m, t; k_1), X_2(n, t; k_2)$ to the matrix equation

$$AX_1 = \begin{bmatrix} X_2 \\ 0 \end{bmatrix}, \quad (3.3)$$

for $\alpha_1 > k_2$ is given by

$$N(m - \alpha_2, t; \beta, k_1, k_2) = g(\beta, t; k_2) L(m - \alpha_2, t; \beta, k_2, k_1),$$

where $g(\beta, t; k_2)$ is given by (2.1) and $L(m - \alpha_2, t; \beta, k_2, k_1)$ is given by (2.3).

PROOF: For A_1, A_2 defined as above we can write (3.3) as the system of equations

$$A_1 X_1 = X_2, \quad (3.4)$$

$$A_2 X_1 = 0. \quad (3.5)$$

Substituting $A_2 = P^{-1} I(s - n, m; \alpha_2) Q^{-1}$ into (3.5) and multiplying on the left by P we obtain

$$I(s - n, m; \alpha_2) Q^{-1} X_1 = 0. \quad (3.6)$$

Let $Q^{-1} X_1 = \text{col}[Y_1, Y_2]$, where $Y_1 = Y_1(\alpha_2, t)$ and $Y_2 = Y_2(m - \alpha_2, t)$. Replacing $Q^{-1} X_1$ in (3.6) by $\text{col}[Y_1, Y_2]$, we have that necessary and sufficient conditions for X_1 to be a solution of (3.6) are that $Y_1 = 0$, $\text{rank } Y_2 = k_1$ and $X_1 = Q \text{col}[0, Y_2]$.

Using this formulation for X_1 in (3.4) gives

$$A_1 Q \begin{bmatrix} 0 \\ Y_2 \end{bmatrix} = X_2. \quad (3.7)$$

Let $A_1 Q = [B_1 \ B_2]$, where $B_1(n, \alpha_2)$ and $B_2 = B_2(n, m - \alpha_2, \beta)$ in (3.7) we then obtain

$$B_2 Y_2 = X_2. \quad (3.8)$$

By Theorem 1 there are $N(m - \alpha_2, t; \beta, k_1, k_2)$ pairs Y_2, X_2 which satisfy (3.8). Since Q is nonsingular there are the same number of pairs X_1, X_2 which satisfy (3.3).

Equations (3.4) and (3.5) represent a special system of two simultaneous equations in the two matrices X_1, X_2 . Very few results seem to exist for such systems. The authors are unable to find the number of solutions to the general system of two simultaneous equations in X_1, X_2 . Such information would allow us to enumerate the ranked solutions to $A_1 X_1 + A_2 X_2 = B$.

THEOREM 3. Let $A_1 = A_1(s, m; r_1)$ and $A_2 = A_2(s, n; r_2)$. Let P_1, Q_1 be nonsingular matrices such that $P_1 A_1 Q_1 = I(s, m; r_1)$. Define $P_1 A_2 = \text{col}[A_{21}, A_{22}]$, where $A_{21} = A_{21}(r, n; \alpha_1)$ and $A_{22} = A_{22}(s - r_1, n; \alpha_2)$. Let P_2, Q_2 be nonsingular matrices such that $P_2 A_{22} Q_2 = I(s - r_1, n; \alpha_2)$. Define $A_{21} Q_2 = [B_1, B_2]$, where $B_2 = B_2(r_1, n - \alpha_2; \beta)$. Then the number of solutions $X_1(m, t; k_1)$, $X_2(n, t; k_2)$ to the matrix equation

$$A_1 X_1 = A_2 X_2, \quad (3.9)$$

is given by

$$N(m, n, t; r_1, r_2, k_1, k_2, \alpha_1, \alpha_2, \beta)$$

$$= \sum_{k_{11}=0}^{\min(\alpha_1, k_1)} G(m, t, r_1; k_1, k_{11}) g(\beta, t; k_{11}) L(n - \alpha_2, t; \beta, k_{11}, k_2),$$

where $G(m, t, r_1; k_1, k_{11})$ can be evaluated using (2.2), $g(\beta, t; k_{11})$ is given by (2.1), and $L(n - \alpha_2, t; \beta, k_{11}, k_2)$ is given by (2.3).

PROOF: The number of solutions to (3.9) is the same as the number of solutions to

$$I(s, m; r_1) X_1 = P_1 A_2 X_2. \quad (3.10)$$

Letting $X_1 = \text{col}[X_{11}, X_{12}]$, $X_{11} = X_{11}(r_1, t; k_{11})$, $X_{12} = X_{12}(m - r_1, t; k_{12})$ and $A = P_1 A_2$, (3.10) becomes

$$AX_2 = \begin{bmatrix} X_{11} \\ 0 \end{bmatrix}. \quad (3.11)$$

Theorem 2 gives the number of pairs X_{11}, X_2 that satisfy (3.11). For each $X_{11}(r_1, t; k_{11})$ the number of $X_{12}(m - r_1, t; k_{12})$ such that $X_1(m, t; k_1) = \text{col}[X_{11}, X_{12}]$ is given by (2.2), denoted by $G(m, t, r_1; k_1, k_{11})$. Therefore the number of solutions X_1, X_2 to (3.9) is given by the product $G(m, t, r_1; k_1, k_{11})g(\theta, t; k_{11})L(n - \alpha_2, t; \beta, k_{11}, k_2)$ summed over the possible values of K_{11} where $K_{11} \leq \alpha_1$ by the hypothesis of Theorem 2.

4. SOME APPLICATIONS.

We can now use Theorem 3 together with some other known results to find the number of solutions $X_1, \dots, X_n, Y_1, \dots, Y_m$ to (1.2) in both the unranked and unranked cases.

THEOREM 4. Let $A_1 = A_1(m, s_0; r_1)$ and $A_2 = A_2(m, t; r_2)$. Let P_1, Q_1 be non-singular matrices such that $P_1 A_1 Q_1 = I(m, s_0; r_1)$. Define $P_1 A_2 = \text{col}[A_{21}, A_{22}]$, where $A_{21} = A_{21}(r_1, t_0; \alpha_1)$ and $A_{22} = A_{22}(m - r_1, t_0; \alpha_2)$. Let P_2, Q_2 be non-singular matrices such that $P_2 A_{22} Q_2 = I(m - r_1, t_0; \alpha_2)$. Define $A_{21} Q_2 = [B_1, B_2]$, where $B_2 = B_2(r_1, t_0 - \alpha_2; \beta)$. Then the number of solutions $X_1(s_0, s_1), \dots, X_n(s_{n-1}, s_n), Y_1(t_0, t_1), \dots, Y_m(t_{m-1}, t_m), m, n \geq 1, s_n = t_m$ to (1.2) is given by

$$\sum_{i_1=0}^{\min(s_0, \dots, s_n)} \sum_{i_2=0}^{\min(t_0, \dots, t_m)} N(s_0, t_0, s_n; r_1, r_2, i_1, i_2, \alpha_1, \alpha_2, \beta) \cdot$$

$$M_n(s_0, \dots, s_n, i_1) M_m(t_0, \dots, t_m, i_2),$$

where $N(s_0, t_0, s_n; r_1, r_2, i_1, i_2, \alpha_1, \alpha_2, \beta)$ can be evaluated using (3.9),

$M_n(s_0, \dots, s_n, i_1)$ and $M_m(t_0, \dots, t_m, i_2)$ can be evaluated using (2.5).

PROOF: Consider the equations

$$A_1 U = A_2 V, \quad (4.1)$$

$$U = X_1 \dots X_n, \quad (4.2)$$

$$V = Y_1 \dots Y_m, \quad (4.3)$$

where $U = U(s_0, s_n; i_1)$, $V = V(t_0, t_m; i_2)$, $0 \leq i_1 \leq \min(s_0, \dots, s_n)$ and

$0 \leq i_2 \leq \min(t_0, \dots, t_m)$. The number of solutions U, V to (4.1) is given by (3.9)

and is represented by $N(s_0, t_0, s_n; r_1, r_2, i_1, i_2, \alpha_1, \alpha_2, \beta)$. The numbers $M_n(s_0, \dots, s_n, i_1)$

and $M_m(t_0, \dots, t_m, i_2)$ represent the number of solutions to (4.2) and (4.3),

respectively, for a fixed U or V . M_n and M_m can be evaluated using (2.5).

The product $\sum_n \sum_m M_n M_m$ summed over the possible ranks of U and V gives the number of solutions to (1.2) in the unranked case.

The next theorem is proved in the same way that Theorem 4 is proved except that we use (2.6) to obtain the number of ranked solutions $X_1, \dots, X_n, Y_1, \dots, Y_m$ to the matrix equations (4.2) and (4.3).

THEOREM 5. Let $A_1, A_2, P_1, Q_1, P_2, Q_2, A_{21}, A_{22}, B_1, B_2, B_{11}, B_{12}, \alpha_1, \alpha_2$, and β be as in Theorem 4. Then the number of solutions

$$X_1(s_0, s_1; j_1), \dots, X_n(s_{n-1}, s_n; j_n), Y_1(t_0, t_1; k_1), \dots, Y_m(t_{m-1}, t_m; k_m), m, n \geq 1,$$

$s_n = t_m$ to (1.2) is given by

$$\sum_{i_1=0}^{\min(j_1, \dots, j_n)} \sum_{i_2=0}^{\min(k_1, \dots, k_m)} N(s_o, t_o, s_n; r_1, r_2, i_1, i_2, \alpha_1, \alpha_2, \beta).$$

$$\cdot T_n(s_o, \dots, s_n; j_1, \dots, j_n, i_1) T_m(t_o, \dots, t_m; k_1, \dots, k_m, i_2),$$

where $N(s_o, t_o, s_n; r_1, r_2, i_1, i_2, \alpha_1, \alpha_2, \beta)$ is evaluated using (3.9) and

$T_n(s_o, \dots, s_n; j_1, \dots, j_n, i_1)$ and $T_m(t_o, \dots, t_m; k_1, \dots, k_m, i_2)$ are evaluated using (2.6).

NOTE: This paper was written while the second named author was on leave at the University of Wyoming.

REFERENCES

- [1] Hodges, John H. Some matrix equations over a finite field, Annali di Matematica 44, (1957) 245-250.
- [2] Hodges, John H. Note on some partitions of a rectangular matrix, Accademia Nazionale Dei Lincei, 8, 39, (1976) 662-666.
- [3] Hodges, John H. Ranked partitions of rectangular matrices over finite fields, Accademia Nazionale Dei Lincei, 8, 60, (1976) 6-12.
- [4] Landsberg, Georg. Über eine Anzahlbestimmung und eine angewandte Mathematik, III, (1893) 87-88.
- [5] Porter, Duane A. The matrix equation $AX_1 + \dots + X_a = B$, Accademia Nazionale Dei Lincei, 8, 44, (1968) 727-732.
- [6] Porter, Duane A. The matrix equation $A_1X_1 + \dots + A_mX_m = B$ in $GF(q)$, Journal of Natural Sciences and Mathematics, 13, 1, (1973) 115-124.

- [7] Porter, Duane A. Some partitions of a rectangular matrix, Accademia Nazionale Dei Lincei, 9, 56, (1974) 667-671.
- [8] Porter, Duane A. Solvability of the matrix equation $AX = B$, Linear Algebra and its Applications, 15, (1978).
- [9] Porter, Duane A., and Nick Mousouris, Ranked solutions of $AXC = B$ and $AX = B$, Linear Algebra and its Applications, 6, (1978) 153-159.
- [10] Porter, Duane A., and Nick Mousouris, Ranked solutions to some matrix equations, Linear and Multilinear Algebra, 6, (1978) 153-159.
- [11] Porter, Duane A., and A. Allan Riveland, A generalized skew equation over a finite field, Mathematische Nachrichten, 69, (1971) 291-296.