Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Ronald H. Dalla, A. Duane Porter

A Consideration by Rank of the Matrix Equation $AX_1 \cdots X_n = B$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **52** (1972), n.3, p. 301–311.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_52_3_301_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1972.

Algebra. — *A Consideration by Rank of the Matrix Equation* $AX_1 \cdots X_n = B$. Nota di RONALD H. DALLA e A. DUANE PORTER, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Si determina il numero delle soluzioni di certi tipi dell'equazione matriciale $AX_1 \cdots X_n = B$ sopra un campo di Galois, nonché il numero delle partizioni di una data matrice B in una somma di matrici ottenibili ciascuna sotto la forma $AX_1 \cdots X_n$.

1. INTRODUCTION

Let GF(q) denote the finite field with $q = p^f$ elements, p a prime. Elements of GF(q) will be denoted by Roman letters $a, b, c, \cdots$. Matrices with elements from GF(q) will be denoted by Roman capitals $A, B, \cdots$. $A(n, s)$ 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 will denote the identity matrix of order r, and $I(n, s; r)$ will denote a matrix of n rows and s columns having I_r in its upper left hand corner and zeros elsewhere.

Let $A = A(s, m; r)$ and $B = B(s, t; \omega)$ with $\omega \leq r$. John H. Hodges [3] determined the number of matrices $X = X(m, t)$ over GF(q) such that $AX = B$. A. Duane Porter [8] found the number of solutions $X_1(s, s_1)$, $X_i(s_{i-1}, s_i)$, $1 < i < a$, $X_a(s_{a-1}, t)$ over GF(q) of the matrix equation $AX_1 \cdots X_a = B$, with A, B defined as above, $a \geq 2$, and where s_i, $1 \leq i < a$ represents an arbitrary positive integer. We are considering the same type of problem as A. Duane Porter did in [8], but we are finding the number of solutions of fixed ranks. John H. Hodges considered similar problems of fixed ranks in [4] and [5].

We seek the number $N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$ of matrices $X_1(m, t_1; k_1)$, $X_i(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $X_n(t_{n-1}, t; k_n)$ over GF(q) such that

$$AX_1 \cdots X_n = B, \tag{1.1}$$

where $A=A(s,m;s)$, $B=B(s,t;\omega)$, $n\geq 2$, and $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$. As a corollary to our main result we will also obtain the number $M = M(C, D, k_1, t_2, \cdots, t_{n-1}, k_n)$ of solutions $Y_1(t, t_{n-1}; k_n)$, $Y_i(t_{n-i+1}, t_{n-i}; t_{n-i+1})$, $2 \leq i \leq n-1$, $Y_n(t_1, m; k_1)$ over GF(q) of the matrix equation

$$Y_1 \cdots Y_n C = D, \tag{1.2}$$

where $C=C(m, s; s)$, $D=D(t, s; \omega)$, $n\geq 2$ and $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$.

(*) Nella seduta dell'11 marzo 1972.

First (Theorem 1) a formula is proved which gives $N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$ as a sum involving the numbers $N'(I_s, B_0, r_1, t_2, \cdots, t_{n-1}, k_n)$, where $s = \text{rank}(A)$; B_0 is the canonical form for B under equivalence of matrices and r_1 runs from $\max(\omega, k_1 - m + s)$ to $\min(k_1, s)$. Then (Theorem 2) the number $N'(I_s, B_0, r_1, t_2, \cdots, t_{n-1}, k_n)$ is found in terms of certain exponential sums $H(s, t, \omega; z)$ whose explicit values are known [2, § 8]. We then combine Theorems 1 and 2 to obtain the main result, which is the value of $N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$. Finally, in § 5, we consider the number of partitions of a matrix B into a sum of h matrix products, where each product is in the form of the left side of (1.1).

The methods employed here are similar to those used in [8] and [9] in the treatment of problems that are similar to the ones that we are now discussing.

2. Notation and Preliminaries

If $A = A(n, n) = (a_{ij})$, then $\sigma(A) = \sum_{i=1}^{n} a_{ii}$ is the trace of A. It is easily shown that if $A = A(n, n)$, $B = B(n, n)$ and C and D are such that CD is square then $\sigma(A + B) = \sigma(A) + \sigma(B)$ and $\sigma(DC) = \sigma(CD)$.

For $c \in GF(q)$, we define

$$e(c) = \exp(2\pi i t(c)/p) \quad ; \quad t(c) = c + c^p + \cdots + c^{p^{f-1}}, \tag{2.1}$$

from which it follows that

$$e(c + b) = e(c)\, e(b) \quad \text{and} \quad \sum_b e(cb) = \begin{cases} q, & (c = 0) \\ 0, & (c \neq 0), \end{cases} \tag{2.2}$$

where the sum is over all $b \in GF(q)$. By use of (2.2), we may show that for $B = B(m, n)$

$$\sum_C e\{\sigma(BC)\} = \begin{cases} q^{mn}, & (B = 0), \\ 0, & (B \neq 0), \end{cases} \tag{2.3}$$

where the sum is over all $C = C(n, m)$. The number of $s \times t$ matrices of rank r is given by Landsberg [6] to be

$$g(s, t, r) = q^{r(r-1)/2} \prod_{i=1}^{r} \frac{(q^{s-i+1} - 1)(q^{t-i+1} - 1)}{(q^i - 1)}, \; r > 1, \tag{2.4}$$

$$g(s, t, 0) = 1.$$

In particular the number of nonsingular matrices of order m is given by

$$g_m = g(m, m, m). \tag{2.5}$$

Following [2, (8.4)], if $B = B(s, t; \omega)$, we define

$$H(B, z) = \sum_C e\{-\sigma(BC)\}, \tag{2.6}$$

where the summation is over all $C = C(t, s; z)$. This sum is evaluated [2, Theorem 7] to be

$$(2.7) \quad H(B, z) = q^{\omega z} \sum_{j=0}^{z} (-1)^j q^{j(j-2\omega-1)/2} \begin{bmatrix} \omega \\ j \end{bmatrix} g(s-\omega, t-\omega, z-j),$$

where the bracket in (2.7) denotes the q–binomial coefficient defined for nonnegative integers ω and j by

$$\begin{bmatrix} \omega \\ 0 \end{bmatrix} = 1, \begin{bmatrix} \omega \\ j \end{bmatrix} = \prod_{i=0}^{j-1} \frac{(1-q^{\omega-i})}{(1-q^{i+1})} \text{ if } 1 \leq j \leq \omega, \begin{bmatrix} \omega \\ j \end{bmatrix} = 0 \text{ if } j > \omega,$$

and $g(s-\omega, t-\omega, z-j)$ is given by (2.4). From (2.7) it is clear that $H(B, z)$ depends only upon the integers s, t, ω and z so we write $H(B, z) = H(s, t, \omega; z)$.

Let $A = A(n, n)$. Then, in view of the definition of trace $-\sigma(A) = \sigma(-A)$. Therefore, by (2.6), for $B = B(s, t; \omega)$ and $C = C(t, s; z)$,

$$\sum_C e\{\sigma(BC)\} = \sum_C e\{-(-\sigma(BC))\} = \sum_C e\{-\sigma(-BC)\} =$$

$$= \sum_C e\{-\sigma((-B)C)\} = H(-B, z).$$

But $-B = -B(s, t; \omega)$ and since from (2.7) it is clear that $H(-B, z)$ depends only upon the integers s, t, ω, and z, we get that $H(-B, z) = H(B, z)$. Therefore,

$$(2.8) \qquad \sum_C e\{\sigma(BC)\} = H(B, z) = H(s, t, \omega; z),$$

where the summation is over all $C = C(t, s; z)$.

3. Some useful results

The following results are necessary to some of the proofs of this paper and are included for completeness.

LEMMA 1. *Let* $D = D(t, s)$ *be partitioned as* $D = col(D_1, D_2)$ *where* $D_1 = D_1(k, s)$ *and* $D_2 = D_2(t-k, s)$. *For* $1 \leq i \leq n-2$ *let* S_i *be a nonsingular matrix of order* t_{i+1}. *For* $1 \leq i \leq n-3$ *partition* S_i *as* (S_{i1}, S_{i2}) *where* $S_{i1} = S_{i1}(t_{i+1}, t_{i+2}; t_{i+2})$ *and* $S_{i2} = S_{i2}(t_{i+1}, t_{i+1}-t_{i+2}; t_{i+1}-t_{i+2})$. *Finally, partition* S_{n-2} *as* $(S_{n-2,1}, S_{n-2,2})$ *where* $S_{n-2,1} = S_{n-2,1}(t_{n-1}, k; k)$ *and* $S_{n-2,2} = S_{n-2,2}(t_{n-1}, t_{n-1}-k; t_{n-1}-k)$. *Then*

$$col(S_{11} \cdots S_{n-2,1} D_1, 0) = I(t_1, t_2; t_2) S_{11} \cdots I(t_{n-2}, t_{n-1}; t_{n-1}) S_{n-2} I(t_{n-1}, t; k) D,$$

where 0 *denotes a zero matrix of size* $(t_1 - t_2) \times s$.

The proof of Lemma 1 is given in [1, Lemma 2].

LEMMA 2. *For any matrix* $A(s, t_0; k)$,

$$\sum_{Z_1,\cdots,Z_n} e\{\sigma(AZ_1 \cdots Z_n)\} = \left(\left[\prod_{i=1}^{n} g(t_{i-1}, t_i, k_i)\right] \Big/ \prod_{j=0}^{n} g_{t_j}\right) \cdot$$

$$\sum_{R_1,S_1,\cdots,S_{n-1},Q_n} e\{\sigma(AR_1 I(t_0, t_1; k_1) S_1 \cdots S_{n-1} I(t_{n-1}, t_n; k_n) Q_n^{-1})\},$$

where the summations are over all $Z_i(t_{i-1}, t_i; k_i)$, $1 \leq i \leq n$, $R_1(t_0, t_0; t_0)$, $S_j(t_j, t_j; t_j)$, $1 \leq j \leq n-1$, *and* $Q_n(t_n, t_n; t_n)$. R_1, S_j, $1 \leq j \leq n-1$, *and* Q_n *are determined by writing* Z_1, Z_i, $1 \leq i \leq n-1$, *and* Z_n, *respectively, in their canonical forms under equivalence* [7, *Theorem* 3.7]. *The value of* $g(s, t, r)$ *is given explicitly by* (2.4).

The proof of Lemma 2 is given in [1, Lemma 3].

LEMMA 3. *Let* D *and* S_i, $1 \leq i \leq n-2$, *be as in Lemma* 1. *Then*

$$\sum_{S_1} \cdots \sum_{S_{n-2}} \sum_{Z_1} e\{\sigma(Z_1 \operatorname{col}(S_{11} \cdots S_{n-2,1} D_1, 0))\} = \left(\prod_{i=2}^{n-1} g_{t_i}\right) H(t_1, s, r; k_1),$$

where $r = rank(D_1)$, $0 \leq r \leq min(k, s)$, *and the summations are over all* $Z_1 = Z_1(s, t_1; k_1)$ *and all nonsingular* S_i *of order* t_{i+1}, $1 \leq i \leq n-2$. $H(t_1, s, r; k_1)$ *is given by* (2.7) *and* (2.8). *The value of* g_{t_i} *is given explicitly by* (2.4) *and* (2.5) *and* 0 *denotes a zero matrix of size* $(t_1 - t_2) \times s$.

The proof of Lemma 3 is also given in [1, Lemma 4].

4. THE MAIN THEOREMS

If $A = A(s, m; s)$ and $B = B(s, t; \omega)$, let $N = N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$ denote the number of solutions $X_1(m, t_1; k_1)$, $X_i(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $X_n(t_{n-1}, t; k_n)$, with $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$ and $n \geq 2$, of the matric equation (1.1). If we take A and B in their canonical forms under equivalence [7, Theorem 3.7], we obtain the equivalent equation

$$RI(s, m; s) X_1 \cdots X_n = I(s, t; \omega) = B_0, \tag{4.1}$$

where R is a fixed nonsingular matrix of order s. Partition X_1 as $X_1 = \operatorname{col}(X_{11}, X_{12})$ where $X_{11} = X_{11}(s, t_1)$ and $X_{12} = X_{12}(m - s, t_1)$. Then (4.1) simplifies to

$$RX_{11} X_2 \cdots X_n = B_0, \tag{4.2}$$

which is clearly independent of X_{12}. A detailed consideration of (4.2) and its relationship to (4.1) and thus to (1.1) leads us to the next Theorem.

THEOREM 1. *Let* $A = A(s, m; s)$ *and* $B = B(s, t; \omega)$. *Then the number* $N = N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$ *of solutions* X_i, $1 \leq i \leq n$, *with* $\omega \leq min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$, *of* (1.1) *is given by the reduction formula*

$$N = \sum_{r_1=\rho_1}^{\min(s,k_1)} q^{r_1(m-s)} g(m - s, t_1 - r_1, k_1 - r_1) N', \tag{4.3}$$

where $B_0 = I(s, t; \omega)$, $\rho_1 = \max(\omega, k_1 - m + s)$, $n \geq 2$, *and* X_i, $1 \leq i \leq n$, *is as defined above* (4.1). $N' = N'(I_s, B_0, r_1, t_2, \cdots, t_{n-1}, k_n)$ *is the number of solutions* $X_{11}, X_i, 2 \leq i \leq n-1, X_n$, *of* (4.2) *of fixed ranks* r_1, t_i, $2 \leq i \leq n-1$, k_n, *respectively, with* $\rho_1 \leq r_1 \leq \min(s, k_1)$. X_{11} *is defined above* (4.2) *and* $g(s, t, r)$ *is given explicitly by* (2.4).

Proof. Let r_1 be an arbitrary integer such that $\rho_1 \leq r_1 \leq \min(s, k_1)$ with $\rho_1 = \max(\omega, k_1 - m + s)$. Let X_{11}, X_i, $2 \leq i \leq n$, be an arbitrary solution of (4.2) of ranks r_1, t_i, $2 \leq i \leq n-1$, k_n, respectively. Then the number of associated solutions $X_1 = \mathrm{col}(X_{11}, X_{12})$, X_i, $2 \leq i \leq n$, of (4.1) of ranks k_1, t_i, $2 \leq i \leq n-1$, k_n, respectively, is just the number of choices of $X_{12}(m-s, t_1)$ for which X_1 has rank k_1. The number of choices of X_{12} is given by A. Allan Riveland [10] to be

$$q^{r_1(m-s)} g(m-s, t_1 - r_1, k_1 - r_1). \tag{4.4}$$

Every solution X_i, $1 \leq i \leq n$, of (4.1) is associated with a unique solution X_{11}, X_i, $2 \leq i \leq n$, of (4.2) and the number of X_i, $1 \leq i \leq n$, produced by a fixed X_{11}, X_i, $2 \leq i \leq n$, is given by (4.4), the latter expression depending only on the rank of X_{11}. Thus, if we multiply the number of solutions of (4.2) of fixed ranks r_1, t_i, $2 \leq i \leq n-1$, k_n, respectively, by (4.4) and sum over all $\rho_1 \leq r_1 \leq \min(s, k_1)$, we obtain the number of solutions of (4.1) and so equivalently of (1.1). The resulting formula is (4.3) so the Theorem is proved.

In view of Theorem 1, to find N we must be able to find the number $N' = N'(I_s, B_0, r_1, t_2 \cdots, t_{n-1}, k_n)$ of solutions $X_{11}(s, t_1; r_1)$, $X_i(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $X_n(t_{n-1}, t; k_n)$ of (4.2). Since R is a fixed nonsingular matrix of order s, then if we let $RX_{11} = Z_{11}(s, t_1; r_1)$, (4.2) is equivalent to

$$Z_{11} X_2 \cdots X_n = I(s, t; \omega) = B_0. \tag{4.5}$$

THEOREM 2. *Let* $B_0 = I(s, t; \omega)$. *Then the number* $N' = N'(I_s, B_0, r_1, t_2, \cdots, t_{n-1}, k_n)$ *of solutions* $X_{11}(s, t_1; r_1)$, $X_i(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $X_n(t_{n-1}, t; k_n)$, of (4.2), *where* $\omega \leq \min(s, r_1, t_2, \cdots, t_{n-1}, k_n)$, *is given by*

$$N' = [g(t-\omega, t-k_n, t-k_n)/g_t q^{sk_n}] g(t_{n-1}, t, k_n) \cdot \prod_{j=1}^{n-2} g(t_j, t_{j+1}, t_{j+1}) \prod_{i=1}^{k_n} (q^t - q^{t-i}) \sum_{r=0}^{\min(k_n, s)} H(t_1, s, r; r_1) H(s, k_n, \omega; r), \tag{4.6}$$

where $g(m, t, r)$ *is given explicitly by* (2.4) *and* $H(s, t, \omega; z)$ *is given in terms of* $g(m, t, r)$ *by* (2.7) *and* (2.8). *The product over* j *is defined as* 1 *if* $n = 2$ *and the product over* i *is defined as* 1 *if* $k_n = 0$.

Proof. In [1, Theorem 1], we found the number of solutions $Y_1(s, t_1; k_1)$, $Y_1(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $Y_n(t_{n-1}, t; k_n)$, of the matrix equation $Y_1 \cdots Y_n = B$, with $B = B(s, t; \omega)$ and $\omega \leq \min(k_1, t_2, \cdots, t_{n-1}, k_n)$. But if we make the substitution $k_1 = r_1$, $Z_{11} = Y_1$ and $X_i = Y_i$, $2 \leq i \leq n$, then (4.5), and hence (4.2), is equivalent to the matrix equation $Y_1 \cdots Y_n = B$.

Therefore we have found the number of solutions of (4.2) and (4.6) is the result that [1, Theorem 1] gives us.

Now, by combining the two previous Theorems, we obtain the desired result.

THEOREM 3. *Let* $A = A(s, m; s)$ *and* $B = B(s, t; \omega)$. *Then the number* $N = N(A, B, k_1, t_2, \cdots, t_{n-1}, k_n)$ *of solutions* $X_1(m, t_1, k_1)$, $X_i(t_{i-1}, t_i; t_i)$, $2 \leq i \leq n-1$, $X_n(t_{n-1}, t, k_n)$, *with* $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$ *and* $n \geq 2$, *of the matrix equation* (1.1), *is given by*

$$(4.7) \quad N = [g(t_{n-1}, t, k_n) g(t-\omega, t-k_n, t-k_n)/g_t q^{sk_n}] \prod_{j=1}^{n-2} g(t_j, t_{j+1}, t_{j+1}) \prod_{i=1}^{k_n} (q^t - q^{t-i}) \cdot$$

$$\cdot \sum_{r_1=\rho_1}^{\min(s, k_1)} \left[q^{r_1(m-s)} g(m-s, t_1-r_1, k_1-r_1) \sum_{r=0}^{\min(k_n, s)} H(t_1, s, r; r_1) H(s, k_n, \omega; r) \right],$$

where $\rho_1 = \max(\omega, k_1 - m + s)$ *and* r_1 *is the rank of* X_{11} *with* $\rho_1 \leq r_1 \leq \min(s, k_1)$. X_{11} *is as previously defined in the sentences following* (4.1). $g(m, t, r)$ *is given explicitly by* (2.4) *and* $H(s, t, \omega; z)$ *is given in terms of* $g(m, t, r)$ *by* (2.7) *and* (2.8). *The product over* i *is defined as* 1 *if* $k_n = 0$ *and the product over* j *is defined as* 1 *if* $n = 2$.

Now we will determine the number $M = M(C, D, k_1, t_2, \cdots, t_{n-1}, k_n)$ of solutions $Y_1(t, t_{n-1}, k_n)$, $Y_i(t_{n-i+1}, t_{n-i}, t_{n-i+1})$, $2 \leq i \leq n-1$, $Y_n(t_1, m; k_1)$ of (1.2), with $C = C(m, s; s)$, $D = D(t, s; \omega)$, $n \geq 2$ and $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$. Equation (1.2) is equivalent to the matrix equation

$$(4.8) \qquad C' Y'_n \cdots Y'_1 = D'.$$

But (4.8) and (1.1) are equivalent so the following corollary is a direct consequence of Theorem 3.

COROLLARY 1. *Let* $C = C(m, s; s)$ *and* $D = D(t, s; \omega)$. *Then the number* $M = M(C, D, k_1, t_2, \cdots, t_{n-1}, k_n)$ *of solutions* $Y_1(t, t_{n-1}; k_n)$, $Y_i(t_{n-i+1}, t_{n-i}; t_{n-i+1})$, $2 \leq i \leq n-1$, $Y_n(t_1, m; k_1)$ *of the matrix equation* (1.2), *with* $\omega \leq \min(s, k_1, t_2, \cdots, t_{n-1}, k_n)$ *and* $n \geq 2$, *is given by* (4.7).

5. THE GENERAL PARTITION

Let $B = B(s; t; \omega)$. For $1 \leq k \leq h$, let $A_k = A_k(s, m_k; s)$, $X_{k,1} = X_{k,1}(m_k, t_{k,1}; j_{k,1})$, $X_{k,i} = X_{k,i}(t_{k,i-1}, t_{k,i}; t_{k,i})$, $2 \leq i \leq n_k - 1$, and $X_{k,n_k} = X_{k,n_k}(t_{k,n_k-1}, t; \mu)$. We seek the number of ways $B(s, t; \omega)$ may be partitioned as

$$(5.1) \qquad \sum_{k=1}^{h} (A_k X_{k,1} \cdots X_{k,n_k}) = B,$$

where the matrices appearing in (5.1) are such that the matrices can satisfy (5.1). If we take A_k, $1 \leq k \leq h$, and B in their canonical forms under equivalence [7, Theorem 3.7], we obtain the equivalent matrix equation

$$\sum_{k=1}^{h} (R_k \, I(s, m_k; s) \, X_{k,1} \cdots X_{k,n_k} = B_0, \tag{5.2}$$

where $B_0 = I(s, t; \omega)$ and where for each k, $1 \leq k \leq h$, R_k is a fixed non-singular matrix of order s. For each k, $1 \leq k \leq h$, partition $X_{k,1}$ as $X_{k,1} = \mathrm{col}(Z_{k,1}, Z_{k,2})$ with $Z_{k,1} = Z_{k,1}(s, t_{k,1})$ and $Z_{k,2} = Z_{k,2}(m_k - s, t_{k,1})$. Then (5.2) may be simplified to

$$\sum_{k=1}^{h} (R_k \, Z_{k,1} \, X_{k,2} \cdots X_{k,n_k}) = B_0, \tag{5.3}$$

which is clearly independent of $Z_{k,2}$ for each k, $1 \leq k \leq h$. A detailed consideration of (5.3) and its relationship to (5.2) and thus to (5.1) leads us to the following Theorem.

THEOREM 4. *Let* $B = B(s, t; \omega)$. *For* $1 \leq k \leq h$, *let* A_k *and* $X_{k,i}$, $1 \leq i \leq n_k$, *be as defined above* (5.1). *Then the number* $\bar{N}$ *of ways* B *can be partitioned as in* (5.1) *is given by the reduction formula*

$$\bar{N} = \sum_{r_{k,1} = \rho_{k,1}}^{\min(s, j_{k,1})} \left(\left[\prod_{k=1}^{h} q^{r_{k,1}(m_k - s)} \, g(m_k - s, t_{k,1} - r_{k,1}, j_{k,1} - r_{k,1}) \right] \bar{M}_h \right), \tag{5.4}$$

where for $1 \leq k \leq h$, $\rho_{k,1} = \max(0, j_{k,1} - m_k + s)$. *For* $1 \leq k \leq h$, $r_{k,1}$ *is the rank of* $Z_{k,1}$, *with* $\rho_{k,1} \leq r_{k,1} \leq \min(j_{k,1}, s)$. $\bar{M}_h$ *is the number of solutions of* (5.3) *of fixed ranks* $r_{k,1}, t_{k,i}$, $2 \leq i \leq n_k - 1$, *and* μ, *for* $1 \leq k \leq h$. $g(s, t, \beta)$ *is given explicitly by* (2.4). *The summation in* (5.4) *indicates a summation over all possible* $r_{k,1}$ *with* $\rho_{k,1} \leq r_{k,1} \leq \min(s, j_{k,1})$ *and* $1 \leq k \leq h$.

Proof. For each k, $1 \leq k \leq h$, let $r_{k,1}$ be an arbitrary integer such that $\rho_{k,1} \leq r_{k,1} \leq \min(s, j_{k,1})$ with $\rho_{k,1}$ as described in the theorem. Let $Z_{k,1}, X_{k,i}$, $2 \leq i \leq n_k - 1$; X_{k,n_k}, $1 \leq k \leq h$, be an arbitrary solution of (5.3) of ranks $r_{k,1}, t_{k,i}$, $2 \leq i \leq n_k - 1$; μ, $1 \leq k \leq h$, respectively. Then the number of associated solutions $X_{k,1}, X_{k,i}$, $2 \leq i \leq n_k - 1$; X_{k,n_k}, $1 \leq k \leq h$, of (5.2) of ranks $j_{k,1}, t_{k,i}$, $2 \leq i \leq n_k - 1$; μ, $1 \leq k \leq h$, respectively, is just the number of choices of $Z_{k,2}$ for which $X_{k,1}$ has rank $j_{k,1}$, $1 \leq k \leq h$.

Fix k, $1 \leq k \leq h$. Then, proceeding in the same manner as A. Allan Riveland [10] did to obtain a similar result, we find that the number of $X_{k,1}, X_{k,i}$, $2 \leq i \leq n_k - 1$; X_{k,n_k} produced by a fixed $Z_{k,1}, X_{k,i}$, $2 \leq i \leq n_k - 1$; X_{k,n_k} is given by

$$H_k = q^{r_{k,1}(m_k - s)} \, g(m_k - s, t_{k,1} - r_{k,1}, j_{k,1} - r_{k,1}), \tag{5.5}$$

where $g(s, t, \beta)$ is given explicitly by (2.4).

Therefore, the number of $X_{k,1}, X_{k,i}, 2 \leq i \leq n_k - 1$; $X_{k,n_k}, 1 \leq k \leq h$, produced by a fixed $Z_{k,1}, X_{k,i}, 2 \leq i \leq n_k - 1$; $X_{k,n_k}, 1 \leq k \leq h$, is given by

$$\prod_{k=1}^{h} H_k . \tag{5.6}$$

Thus, if we multiply (5.6) by the number $\bar{M}_h$ of solutions of (5.3) of fixed ranks $r_{k,1}, t_{k,i}, 2 \leq i \leq n_k - 1$; μ, $1 \leq k \leq h$, and sum over all $r_{k,1}$ such that $\rho_{k,1} \leq r_{k,1} \leq \min(s, j_{k,1})$ and $1 \leq k \leq h$, we obtain the total number of solutions of (5.2) and so equivalently of (5.1). But if we do this the resulting formula is (5.4) so the Theorem is proved.

The next Theorem gives us the value of $\bar{M}_h$.

THEOREM 5. *Let* $B_0 = I(s, t; \omega)$. *Then, for* $1 \leq k \leq h$, *the number* $\bar{M}_h$ *of solutions* $Z_{k,1}(s, t_{k,1}; r_{k,1})$, $X_{k,i}(t_{k,i-1}, t_{k,i}; t_{k,i})$, $2 \leq i \leq n_k - 1$, $X_{k,n_k}(t_{k,n_k-1}, t; \mu)$ *of* (5.3) *is given by*

$$\bar{M}_h = q^{-st} \sum_{z=0}^{\min(s,t)} H(s, t, \omega; z) \prod_{k=1}^{h} g(t_{k,n_k-1}, t, \mu) \cdot \tag{5.7}$$

$$\cdot \left(\prod_{i=1}^{n_k-2} g(t_{k,i}, t_{k,i+1}, t_{k,i+1}) \right) H(t_{k,1}, s, \tau_k, r_{k,1}),$$

where $\rho_{k,1} \leq r_{k,1} \leq \min(s, j_{k,1})$ *and* $\rho_{k,1} = \max(0, j_{k,1} - m_k + s)$. $g(s, t, \omega)$ *is given explicitly by* (2.4) *and* $H(e, f, j; \rho)$ *is given in terms of* $g(s, t, \omega)$ *by* (2.7) *and* (2.8). *The product over i is defined as* 1 *if* $n_k = 2$, *for* $1 \leq k \leq h$.

Proof. Let $B_0 = I(s, t; \omega)$. For $1 \leq k \leq h$, let $P_k(X_k) = R_k Z_{k,1} X_{k,2} \cdots X_{k,n_k}$. Then, in view of (2.3), $\bar{M}_h$ may be expressed as

$$\bar{M}_h = q^{-st} \sum_{Z_{k,1}, X_{k,j}} \sum_{C} e \left\{ \sigma \left[\left(\sum_{b=1}^{h} P_b(X_b) \right) - B_0 C \right] \right\},$$

where the sum over $Z_{k,1}, X_{k,j}$ indicates a summation over each $Z_{k,1}, X_{k,j}$, $2 \leq j \leq n_k$, $1 \leq k \leq h$, as these matrices are defined above, and the sum over C is over all $C = C(t, s)$. By use of the properties of the exponential function and the trace of a matrix given in Section 2, by (2.2), and since the sum over $Z_{i,1}, X_{i,j}$ is distinct for each i, $1 \leq i \leq h$, we obtain

$$\bar{M}_h = q^{-st} \sum_{C} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} \sum_{Z_{k,1}, X_{k,2}, \cdots, X_{k,n_k}} e\{\sigma(R_k Z_{k,1} X_{k,2} \cdots X_{k,n_k} C)\}.$$

Now for each k, $1 \leq k \leq h$, R_k is a fixed nonsingular matrix of order s. For each k, $1 \leq k \leq h$, as $Z_{k,1}$ runs through all $Z_{k,1}(s, t_{k,1}; r_{k,1})$, $R_k Z_{k,1}$ also runs through all $Z_{k,1}(s, t_{k,1}; r_{k,1})$ in some order. Therefore, since $\sigma(AB) = \sigma(BA)$ for AB square, we have that

$$\bar{M}_h = q^{-st} \sum_{C} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} \sum_{Z_{k,1}, X_{k,2}, \cdots, X_{k,n_k}} e\{\sigma(C Z_{k,1} X_{k,2} \cdots X_{k,n_k})\}.$$

For $1 \leq k \leq h$, let

$$U_k = \left[g(t_{k,n_k-1}, t, \mu)/g_t \prod_{j=1}^{n_k-1} g_{t_{k,j}} \right] \prod_{\delta=1}^{n_k-2} g(t_{k,\delta}, t_{k,\delta+1}, t_{k,\delta+1}).$$

Then, by Lemma 2 and the fact that $\sigma(AB) = \sigma(BA)$ for AB square, we obtain

$$\bar{M}_h = q^{-st} \sum_{C} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} U_k \sum_{Z_{k,1}, T_{k,1}, S_{k,1}, \cdots, S_{k,n_k-2}, Q_{k,n_k}} e\{\sigma(Z_{k,1} T_{k,1} \cdot$$

$$\cdot I(t_{k,1}, t_{k,2}; t_{k,2}) S_{k,1} \cdots S_{k,n_k-2} I(t_{k,n_k-1}, t; \mu) Q_{k,n_k}^{-1} C)\},$$

where $T_{k,1}$ is a nonsingular matrix of order $t_{k,1}$ and $S_{k,i}$ is a nonsingular matrix of order $t_{k,i+1}$ for $1 \leq i \leq n_k - 2$. Q_{k,n_k} is a nonsingular matrix of order t that is determined by writing X_{k,n_k} in its canonical form under equivalence [7, Theorem 3.7]. For fixed nonsingular $T_{k,1}$ of order $t_{k,1}$, as $Z_{k,1}$ runs through all $Z_{k,1}(s, t_{k,1}; r_{k,1})$, $Z_{k,1} T_{k,1}$ also runs through all $Z_{k,1}(s, t_{k,1}; r_{k,1})$ in some order. Let $U'_k = U_k g_{t_{k,1}}$. Then, since there are $g_{t_{k,1}}$ such $T_{k,1}$'s, we are led to

$$\bar{M}_h = q^{-st} \sum_{C} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} U'_k \cdot$$

$$\cdot \sum_{Z_{k,1}, S_{k,1}, \cdots, S_{k,n_k-2}, Q_{k,n_k}} e\{\sigma(Z_{k,1} I(t_{k,1}, t_{k,2}; t_{k,2}) S_{k,1} \cdots S_{k,n_k-2} I(t_{k,n_k-1}, t; \mu) Q_{k,n_k}^{-1} C)\}.$$

We now divide the sum over C into successive sums over all $C(t, s; z)$ for $0 \leq z \leq \min(s, t)$, and obtain the following for $\bar{M}_h$.

$$\bar{M}_h = q^{-st} \sum_{z=0}^{\min(s,t)} \sum_{C(t,s;)} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} U'_k \cdot$$

$$\cdot \sum_{Z_{k,1}, S_{k,1}, \cdots, S_{k,n_k-2}, Q_{k,n_k}} e\{\sigma(Z_{k,1} I(t_{k,1}, t_{k,2}; t_{k,2}) S_{k,1} \cdots S_{k,n_k-2} I(t_{k,n_k-1}, t; \mu) Q_{k,n_k}^{-1} C)\}.$$

For fixed nonsingular Q_{k,n_k} of order t, as C runs through all $C(t, s; z)$, $Q_{k,n_k}^{-1} C$ will also run through all $C(t, s; z)$ in some order. Let $U''_k = U'_k g_t$. Then, since there are g_t such Q_{k,n_k}'s, we have that

$$\bar{M}_h = q^{-st} \sum_{z=0}^{\min(s,t)} \sum_{C(t,s;z)} e\{-\sigma(B_0 C)\} \prod_{k=1}^{h} U''_k \cdot \tag{5.8}$$

$$\cdot \sum_{Z_{k,1}, S_{k,1}, \cdots, S_{k,n_k-2}} e\{\sigma(Z_{k,1} I(t_{k,1}, t_{k,2}; t_{k,2}) S_{k,1} \cdots S_{k,n_k-2} I(t_{k,n_k-1}, t; \mu) C)\}.$$

Fix $C(t, s; z)$. Then for each k, $1 \leq k \leq h$, partition $C(t, s; z)$ as $C(t, s; z) = \operatorname{col}(C_{k,1}, C_{k,2})$ with $C_{k,1} = C_{k,1}(\mu, s)$ and $C_{k,2} = C_{k,2}(t - \mu, s)$.

Then, by Lemma 1, for each k, $1 \leq k \leq h$, the inner sum on the right of (5.8) is equal to

$$(5.9) \qquad \sum_{S_{k,1}} \cdots \sum_{S_{k,n_k-2}} \sum_{Z_{k,1}} e\{\sigma(Z_{k,1} \cdot \mathrm{col}(S_{k,1,1} \cdots S_{k,n_k-2,1} C_{k,1}, 0))\},$$

where, for $1 \leq i \leq n_k - 3$, $S_{k,i} = (S_{k,i,1}, S_{k,i,2})$ with $S_{k,i,1} = S_{k,i,1}(t_{k,i+1}, t_{k,i+2}; t_{k,i+2})$ and where $S_{k,n_k-2} = (S_{k,n_k-2,1}, S_{k,n_k-2,2})$ with $S_{k,n_k-2,1} = S_{k,n_k-2,1}(t_{k,n_k-1}, \mu; \mu)$. O denotes a zero matrix of size $(t_{k,1} - t_{k,2}) \times s$. Now it is clear that

$$(5.10) \qquad \mathrm{rank}(\mathrm{col}(S_{k,1,1} \cdots S_{k,n_k-2,1} C_{k,1}, 0)) = \mathrm{rank}(C_{k,1}).$$

Let rank $(C_{k,1}) = \tau_k$, $0 \leq \tau_k \leq \min(z, \mu)$. Then, by Lemma 3 and (5.10), (5.9) is equal to

$$(5.11) \qquad \left(\prod_{i=2}^{n_k-1} g_{t_{k,i}}\right) H(t_{k,1}, s, \tau_k; r_{k,1}).$$

Thus, by substituting (5.9) and (5.11) into (5.8), we obtain the following for $\bar{M}_h$, where $U_k''' = U_k'' \left(\prod_{i=2}^{n_k-1} g_{t_{k,i}}\right)$.

$$\bar{M}_h = q^{-st} \sum_{z=0}^{\min(s,t)} \sum_{C(t,s;z)} e\{-\sigma(B_0 C)\} \prod_{k=1}^{n} U_k''' H(t_{k,1}, s, \tau_k; r_{k,1}).$$

In view of (2.6) and (2.8),

$$(5.12) \qquad \bar{M}_h = q^{-st} \sum_{z=0}^{\min(s,t)} H(B_0, z) \prod_{k=1}^{h} U_k''' H(t_{k,1}, s, \tau_k; r_{k,1})$$

$$= q^{-st} \sum_{z=0}^{\min(s,t)} H(s, t, \omega; z) \prod_{k=1}^{h} U_k''' H(t_{k,1}, s, \tau_k; r_{k,1}).$$

Thus, if the value of U_k''' is substituted in (5.12), we obtain (5.7) so the Theorem is proved.

The desired result is an immediate consequence of Theorems 4 and 5.

THEOREM 6. *Let* $B = B(s, t; \omega)$. *For* $1 \leq k \leq h$, *let* A_k *and* $X_{k,i}$, $1 \leq i \leq n_k$, *be as defined above* (5.1). *Then the number* $\bar{N}$ *of ways* B *can be partitioned as in* (5.1) *is given by the formula*

$$(5.13) \qquad \bar{N} = \sum_{r_{k,1}=\rho_{k,1}}^{\min(s,j_{k,1})} \left(\left[\prod_{k=1}^{h} q^{r_{k,1}(m_k - s)} g(m_k - s, t_{k,1} - r_{k,1}, j_{k,1} - r_{k,1}) \right] \cdot \right.$$

$$\left. \cdot \left\{ q^{-st} \sum_{z=0}^{\min(s,t)} H(s,t,\omega;z) \prod_{k=1}^{h} \left[g(t_{k,n_k-1}, t, \mu) \left(\prod_{j=1}^{n_k-2} g(t_{k,j}, t_{k,j+1}, t_{k,j+1}) \right) H(t_{k,1}, s, \tau_k; r_{k,1}) \right] \right\} \right),$$

where for $1 \leq k \leq h$, $\rho_{k,1} = \max(0, j_{k,1} - m_k + s)$ *and* $\rho_{k,1} \leq r_{k,1} \leq \leq \min(s, j_{k,1})$. $g(s, t, \beta)$ *is given explicitly by* (2.4) *and* $H(e, f, j; \rho)$ *is given in terms of* $g(s, t, \omega)$ *by* (2.7) *and* (2.8). *The product over* j *is defined as* 1 *if* $n_k = 2$, *for* $1 \leq k \leq h$. *The first summation in* (5.13) *indicates a summation over all possible* $r_{k,1}$ *for* $1 \leq k \leq h$.

REFERENCES

[1] DALLA RONALD H. and A. DUANE PORTER, *The Matrix Equation* $U_1 \cdots U_n A V_1 \cdots \cdots V_m = B$ *Over a Finite Field*, Submitted to «Mathematische Nachrichten».

[2] HODGES JOHN H., *Representations by Bilinear Forms in a Finite Field*, «Duke Mathematical Journal», *22*, 497–510 (1955).

[3] HODGES JOHN H., *The Matric Equation* AX = B *in a Finite Field*, «American Mathematical Monthly», *63*, 243–244 (1956).

[4] HODGES JOHN H., *A Bilinear Matrix Equation Over a Finite Field*, «Duke Mathematical Journal», *31*, 661–666 (1964).

[5] HODGES JOHN H., *A Skew Matrix Equation Over a Finite Field*, «Archiv Der Mathematik», *17*, 49–55 (1966).

[6] LANDSBERG GEORG, *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, «Journal für die reine und angewandte Mathematik», *3*, 87–88 (1893).

[7] PERLIS SAM, *Theory of Matrices*. Addison–Wesley Publishing Company, Inc., Massachusetts, 1958.

[8] PORTER A. DUANE, *The Matric Equation* $AX_1 \cdots X_a = B$, «Accademia Nazionale dei Lincei», *44*, 727–732 (1968).

[9] PORTER A. DUANE, *Generalized Bilinear Forms in a Finite Field*, «Duke Mathematical Journal», *37*, 55–60 (1970).

[10] RIVELAND A. ALLAN, *Counting Solutions to Certain Matrix Equations Over a Finite Field*, Ph. D. Thesis, University of Wyoming, 1972.