MATH. SCAND. 74 (1994), 19–33

COUNTING MATRICES WITH COORDINATES IN FINITE FIELDS AND OF FIXED RANK

DAN LAKSOV[1] and ANDERS THORUP[2]

Abstract.

Over a given finite field, we present a method for obtaining explicit expressions for the number of matrices of given rank satisfying certain conditions. As illustration of the method, we present a series of new formulas, and we obtain simple proofs of known formulas.

Introduction.

We present a method for obtaining explicit expressions for the number of matrices of fixed order and rank with entries in a finite field and satisfying certain additional conditions.

The method is simple and formal and makes it possible to derive many formulas using only standard linear algebra. Applying the method in various examples, we obtain simple proofs of known formulas, and we obtain a series of new formulas. Formulas of this kind have mostly been obtained through the use of recursion and exponential sums. In the references we have listed some articles that illustrate the differences in methods and that are not used elsewhere in the text.

On the other hand, our method explains the appearance of the recursion formulas. Moreover, the expressions obtained from our method are in many cases different from those obtained using exponential sums. As a consequence, we obtain new non-trivial identities between expressions that can be interpreted as special values of certain generalized hypergeometric series.

To illustrate our method, we consider the set of all $m \times t$ matrices and the four subsets defined by the following conditions on the matrix X:

[1] Partially supported by The Göran Gustafsson Foundation for Research in Natural Sciences and Medicine.

[2] Supported in part by the Danish Natural Science Research Council, grant 11–7428.

Received October 6, 1992.

(1) The matrix X is arbitrary,
(2) The rows of the matrix X are non-zero and mutually different,
(3) The matrix X is a solution to the equation $X'SX = 0$ where S is a given regular symmetric $m \times m$ matrix,
(4) The matrix X is a solution to the equation $X'AX = 0$ where A is a given regular antisymmetric $m \times m$ matrix.

Explicit expressions and a recursion formula for the number of all matrices of rank r were given in [Lb]. A recursion formula for the number of matrices of rank r satisfying Condition (2) was obtained by [Ls] and an explicit expression was given in [C3]. Explicit expressions for the number of matrices satisfying Condition (3) or (4) with no condition on the rank were given in [C1, C2]. In the present work we obtain explicit expressions for the subsets of matrices of given rank r. The expressions we derive for the number of all matrices satisfying (3) or (4) are different from those obtained in [C1] and [C2]. Taken in connection with the previous expressions, the new expressions may be seen as a new family of nontrivial identities of hypergeometric series. In fact, these identities led us to the discovery of an error in the expressions obtained in [C2], see Note (6.3) below.

The explicit expressions involve the q-binomial coefficients or Gaussian polynomials,

$$\begin{bmatrix} t \\ r \end{bmatrix} = \frac{(q^t - 1)(q^{t-1} - 1)\dots(q^{t-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1)\dots(q - 1)}.$$

When q is a variable, the expression on the right hand side is in fact a polynomial. In our formulas q will be the number of elements in a finite field. Our method explains the occurrence of these polynomials. In fact, as we show in Section 3, a number of well known properties of the Gaussian polynomials may be obtained on the basis of similar properties of numbers arising from finite dimensional vector spaces over finite fields.

1. Interpolation formulas.

In this section we prove an interpolation formula needed in Section 2. The formula is of Lagrange type, giving the transition between two different bases of the polynomial ring $R[x]$ over a ring R.

DEFINITON 1.1. Let R be a commutative ring with unity. Fix a sequence $\lambda_1, \lambda_2, \dots$ of elements in R, and define polynomials for $r = 0, 1, \dots$

$$Q_r(x) := (x - \lambda_1)(x - \lambda_2)\dots(x - \lambda_r).$$

Then $Q_0(x) = 1$, and the sequence $Q_0(x), Q_1(x), \dots$ forms an R-basis for $R[x]$.

Hence every polynomial $f(x)$ of $R[x]$ uniquely determines coefficients $\begin{bmatrix} f \\ r \end{bmatrix}$ in R for $r = 0, 1, \ldots$ such that

$$f(x) = \sum_{r=0}^{\infty} \begin{bmatrix} f \\ r \end{bmatrix} Q_r(x) \tag{1.1.1}$$

where $\begin{bmatrix} f \\ r \end{bmatrix} = 0$ for $r > \deg f$.

Our notation for the coefficients resembles the usual notation for the q-binomial coefficients. The connection between the two notations will be explained in Remark 1.5 and Note 3.2.

Assume that the differences $\lambda_i - \lambda_j$ are invertible in R whenever $i \neq j$.

PROPOSITION 1.2. *For every polynomial $f(x)$, the following formulas hold,*

$$\begin{bmatrix} f \\ r \end{bmatrix} = \sum_{i=1}^{r+1} \frac{f(\lambda_i)}{Q'_{r+1}(\lambda_i)}, \quad \text{for} \quad r = 0, 1, \ldots \tag{1.2.1}$$

where Q' denotes the formal derivative of the polynomial Q.

PROOF. Clearly, the two sides of (1.2.1) are R-linear maps $R[X] \to R$. Therefore, it suffices to prove that the equations (1.2.1) hold when $f = Q_n$ for $n = 0, 1, \ldots$ Clearly, the left hand side is equal to 1 for $r = n$, and zero otherwise. Consider the right hand side of (1.2.1) for $f = Q_n$. The numerator $Q_n(\lambda_i)$ vanishes when $i \leqq n$. In particular, the right hand side vanishes for $r < n$, and for $r = n$ the only non-vanishing term is equal to 1. Hence it remains to be shown that the right hand side is equal to 0 for $r > n$.

Clearly, it suffices to prove that the right hand side is zero for $r > n$ when the elements $\lambda_{n+1}, \ldots, \lambda_{r+1}$ are independent variables over $\mathbf{Z}$. Set $p = r + 1 - n$, and $x_i := \lambda_{n+i}$ for $i = 1, \ldots, p$. Denote by G the right hand side. Then, after a change of indices,

$$G = \sum_{i=n+1}^{r+1} \frac{Q_n(\lambda_i)}{Q'_{r+1}(\lambda_i)} = \sum_{i=1}^{p} \frac{Q_n(x_i)}{Q'_{r+1}(x_i)}.$$

After a reduction of the fractions in the sum on the right hand side, we obtain the equation,

$$G = \sum_{i=1}^{p} \frac{1}{\prod_{1 \leqq j \leqq p,\, j \neq i} (x_i - x_j)}.$$

It follows that G is symmetric in the p variables $x_1, \ldots, x_p$. Moreover, every denominator on the right hand side divides the Vandermonde determinant $\Delta = \prod_{1 \leqq i < j \leqq p} (x_j - x_i)$. Therefore, the product $G\Delta$ is an alternating polynomial

in $x_1, \ldots, x_p$, and of degree less than the degree of Δ. Consequently, $G = 0$ and we have proved the Proposition.

1.3. Assume for the rest of this section that the sequence of λ_i's consists of the powers of a single element q, that is, $\lambda_i = q^{i-1}$. Then

$$Q_i(x) = (x-1)(x-q)\ldots(x-q^{i-1}). \tag{1.3.1}$$

In this case, the coefficients of the interpolation formula can be expressed by the *q-binomial coefficients*,

$$\begin{bmatrix} r \\ i \end{bmatrix} := \frac{(q^r-1)(q^{r-1}-1)\ldots(q^{r-i+1}-1)}{(q^i-1)(q^{i-1}-1)\ldots(q-1)} \quad \text{for} \quad r, i \geqq 0.$$

For $0 \leqq i \leqq r$, it follows immediately from the definition that

$$\begin{bmatrix} r \\ i \end{bmatrix} = \begin{bmatrix} r \\ r-i \end{bmatrix}. \tag{1.3.2}$$

Moreover,

$$\begin{bmatrix} r \\ i \end{bmatrix} = \frac{Q_i(q^r)}{Q_i(q^i)} = (-1)^i q^{-\binom{i}{2}} \frac{Q_r(q^r)}{Q'_{r+1}(q^{r-i})}, \tag{1.3.3}$$

as follows by an extraction of powers of q and a simple reduction.

PROPOSITION 1.4. *Assume that* $\lambda_i = q^{i-1}$. *Then, for every polynomial* f *and* $r = 0, 1, 2, \ldots$, *the coefficient in the expansion* (1.1.1) *is given by the formulas,*

$$\begin{bmatrix} f \\ r \end{bmatrix} = \sum_{i=0}^{r} \frac{f(q^i)}{Q'_{r+1}(q^i)} = \frac{1}{Q_r(q^r)} \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} f(q^{r-i}).$$

PROOF. The first formula is just a rewriting of (1.2.1), and the second equation follows from Equation (1.3.3).

REMARK 1.5. The formulas apply whenever the element q and the differences $q^i - 1$ for $i > 0$ are invertible. When the latter elements are regular, the formulas can be interpreted in the total ring of fractions of the given ring. In particular, the formulas hold for an element q which is transcendental over a ground ring. Moreover, the formulas for an arbitrary element q follows by specialization from the transcendental case.

Consider the case where q is transcendental. Then the q-binomial coefficients are a priori rational functions of q. It is well known that they are in fact polynomials in q, called the *Gaussian polynomials*. Moreover, the following two formulas are well known,

$$\begin{bmatrix} x^m \\ r \end{bmatrix} = \begin{bmatrix} m \\ r \end{bmatrix}$$

(explaining our choice of notation), and

$$Q_r(x) = \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} x^{r-i}.$$

As we shall see in the Section 3 (Note 3.2 and Remark 3.3), these assertions follow easily from our results.

2. The method.

Let q be a power of a prime number and denote by $\mathbf{F}_q$ the field with q elements. Fix a vectorspace V of finite dimension m over $\mathbf{F}_q$. For a given family $\mathscr{T}$ of subspaces of V, denote by $\mathscr{T}_r$ the set of subspaces of dimension r in the family $\mathscr{T}$. Moreover, for any $t \geqq 0$, denote by

$$\mathrm{Hom}_{\mathscr{T}}(\mathbf{F}_q^t, V) \subseteq \mathrm{Hom}(\mathbf{F}_q^t, V)$$

the set of those linear maps $\mathbf{F}_q^t \to V$ whose image belongs to $\mathscr{T}$. Note that the set $\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)$ consists of the linear maps $\varphi\colon \mathbf{F}_q^t \to V$ such that the rank of φ is equal to r and the image of φ belongs to $\mathscr{T}$. In particular, the set $\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^r, V)$ is the set of injective linear maps $\mathbf{F}_q^r \to V$ whose image belongs to $\mathscr{T}$.

Our method is to combine some simple relations between the numbers of elements in the sets $\mathscr{T}_r$, $\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)$ and $\mathrm{Hom}_{\mathscr{T}}(\mathbf{F}_q^t, V)$ with the interpolation formula obtained in Section 1 with respect to the polynomials

$$Q_i(x) = (x-1)(x-q)\ldots(x-q^{i-1}).$$

When a basis for V is given, $V = \mathbf{F}_q^m$, then $\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)$ is a subset of the set of $m \times t$ matrices, and we obtain the explicit formulas mentioned in the introduction.

PROPOSITION 2.1. *Let $\mathscr{T}$ be a family of linear subspaces of V. Then the cardinalities of the sets $\mathscr{T}_r$, $\mathrm{Hom}_{\mathscr{T}}(\mathbf{F}_q^t, V)$ and $\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)$ are related by the following formulas,*

$$|\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)| = |\mathscr{T}_r| \cdot Q_r(q^t), \tag{2.1.1}$$

$$|\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^t, V)| = \begin{bmatrix} t \\ r \end{bmatrix} \cdot |\mathrm{Hom}_{\mathscr{T}_r}(\mathbf{F}_q^r, V)|, \tag{2.1.2}$$

$$|\mathrm{Hom}_{\mathscr{T}}(\mathbf{F}_q^t, V)| = \sum_{r=0}^{\dim V} |\mathscr{T}_r| \cdot Q_r(q^t). \tag{2.1.3}$$

PROOF. Let U be a subspace of dimension r in V. Clearly, the number of

surjective linear maps $\mathsf{F}_q^t \to U$ is equal to the number of injective linear maps $\mathsf{F}_q^r \to \mathsf{F}_q^t$; hence the number is equal to the product,

$$(q^t - 1)(q^t - q)\dots(q^t - q^{r-1}).$$

In other words, the number is equal to $Q_r(q^t)$, where $Q_r(x)$ is the polynomial of (1.3.1). Therefore, the number $|\mathrm{Hom}_{\mathscr{T}_r}(\mathsf{F}_q^t, V)|$ of linear maps $\mathsf{F}_q^t \to V$ with image in $\mathscr{T}_r$ is the product of $Q_r(q^t)$ and the number of possible images, $|\mathscr{T}_r|$. Hence the first equation holds. The second equation follows by using the first for t and for $t := r$, noting that the quotient $Q_r(q^t)/Q_r(q^r)$ is the q-binomial coefficient $\begin{bmatrix} t \\ r \end{bmatrix}$ by (1.3.3). Finally, the last equation follows from the first by summation over the possible ranks of the subspaces in $\mathscr{T}$.

COROLLARY 2.2. *Considered the polynomial* $f = f_{\mathscr{T}}$ *defined by*

$$f(x) := \sum_{r=0}^{\dim V} |\mathscr{T}_r|\, Q_r(x).$$

Then the following formulas hold:

$$|\mathscr{T}_r| = \begin{bmatrix} f \\ r \end{bmatrix} = \sum_{i=0}^{r} \frac{f(q^i)}{Q'_{r+1}(q^i)}, \tag{2.2.1}$$

$$|\mathrm{Hom}_{\mathscr{T}}(\mathsf{F}_q^t, V)| = f(q^t), \tag{2.2.2}$$

$$|\mathrm{Hom}_{\mathscr{T}_r}(\mathsf{F}_q^r, V)| = \begin{bmatrix} f \\ r \end{bmatrix} Q_r(q^r) = \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} f(q^{r-i}), \tag{2.2.3}$$

$$|\mathrm{Hom}_{\mathscr{T}_r}(\mathsf{F}_q^t, V)| = \begin{bmatrix} f \\ r \end{bmatrix} Q_r(q^t) = Q_r(q^t) \sum_{l=0}^{r} \frac{f(q^i)}{Q'_{r+1}(q^i)} \tag{2.2.4}$$

$$= \begin{bmatrix} t \\ r \end{bmatrix} \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} f(q^{r-i}). \tag{2.2.5}$$

PROOF. By definition of f, the equation (2.2.2) follows from Equation (2.1.3). Moreover, it follows from the definition of the coefficient $\begin{bmatrix} f \\ r \end{bmatrix}$ that $|\mathscr{T}_r| = \begin{bmatrix} f \\ r \end{bmatrix}$. Therefore, the remaining formulas of the Corollary follow from the formulas of Proposition 2.1 and the general expressions for the coefficient $\begin{bmatrix} f \\ r \end{bmatrix}$ in Proposition 1.4.

REMARK 2.3. The Proposition has an obvious dual form. Let $\mathscr{T}^*$ denote the family of polars to the family $\mathscr{T}$, that is, a subspace W of the dual space V^* belongs to $\mathscr{T}^*$, if and only if the intersection of the kernels of the linear forms in

W belongs to $\mathscr{T}$. Clearly, the set of all rank-r linear maps $V \to \mathsf{F}_q^t$ whose kernel belongs to $\mathscr{T}$ corresponds bijectively to the set of all rank-r linear maps $\mathsf{F}_q^t \to V^*$ whose image belongs to $\mathscr{T}^*$. Hence a dual form of the proposition is obtained by applying the proposition to the family $\mathscr{T}^*$ of subspaces in the dual vector space V^*.

3. General matrices.

In this and the following sections the method of Section 2 is illustrated by applying it to the cases mentioned in the introduction. As in Section 2, the vector space V is assumed to be of finite dimension m over the field F_q with q elements.

Let $\mathscr{F}$ be the set of all subspaces of V. Then $\mathrm{Hom}_{\mathscr{F}}(\mathsf{F}_q^t, V)$ is the set of all linear maps $\mathsf{F}_q^t \to \mathsf{F}_q^m$, and $\mathrm{Hom}_{\mathscr{F}_r}(\mathsf{F}_q^r, V)$ is the set $\mathrm{Hom}_r(\mathsf{F}_q^r, \mathsf{F}_q^m)$ of all injective linear maps $\mathsf{F}_q^r \to \mathsf{F}_q^m$. Clearly,

$$|\mathrm{Hom}_r(\mathsf{F}_q^r, \mathsf{F}_q^m)| = Q_r(q^m). \tag{3.0.1}$$

Hence, from Formula (2.1.2), we obtain the following result of Landsberg [Lb].

PROPOSITION 3.1. *The number of $\phi_r(t, m)$ of all $m \times t$ matrices of rank r with entries in F_q is given by the following expressions,*

$$\phi_r(t, m) = |\mathrm{Hom}_r(\mathsf{F}_q^t, \mathsf{F}_q^m)| = \begin{bmatrix} t \\ r \end{bmatrix} \cdot Q_r(q^m) = \frac{Q_r(q^t)Q_r(q^m)}{Q_r(q^r)}.$$

NOTE 3.2. It follows from Equation (2.1.1), or directly, that the number,

$$|\mathscr{F}_r| = \begin{bmatrix} m \\ r \end{bmatrix} = \frac{Q_r(q^m)}{Q_r(q^r)}, \tag{3.2.1}$$

is equal to the number of dimension-r subspaces of V. Clearly, the set $\mathrm{Hom}(\mathsf{F}_q^t, V)$ can be identified with the set of all $m \times t$ matrices, and consequently the cardinality of $\mathrm{Hom}(\mathsf{F}_q^t, V)$ is q^{tm}. Now, let $f = f_{\mathscr{F}} = \sum_{r=0}^{\dim V} \begin{bmatrix} m \\ r \end{bmatrix} Q_r(x)$ be the polynomial of Corollary 2.2. Then it follows from (2.2.2) that $q^{tm} = f(q^t)$. Consequently, since t is arbitrary, it follows that $f(x) = x^m$. From (3.2.1) and the first equation of (2.2.1), we obtain that

$$\begin{bmatrix} x^m \\ r \end{bmatrix} = \begin{bmatrix} m \\ r \end{bmatrix}. \tag{3.2.2}$$

Consider finally Equation (2.2.3). By (3.0.1), or directly, the left hand side of (2.2.3) is $Q_r(q^m)$. The polynomial f on the right hand side of (2.2.3) is $f = x^m$. Therefore, Equation (2.2.3) implies the following equation,

$$Q_r(q^m) = \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} (q^m)^{r-i}.$$

The latter equation holds for all m. Therefore it implies the following equation of polynomials,

$$Q_r(x) = \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} x^{r-i}. \tag{3.2.3}$$

REMARK 3.3. The results of 3.2 were obtained for the given prime power q. However, the results imply corresponding results for an element q which is transcendental over $\mathbf{Z}$. Indeed, when q is transcendental, the q-binomial coefficient $\begin{bmatrix} t \\ r \end{bmatrix}$ is a quotient of polynomials in q with integer coefficients and the denominator is a monic polynomial in q. It follows from the interpretation of (3.2.1) above, that the value of $\begin{bmatrix} t \\ r \end{bmatrix}$ is integral when evaluated on any prime power. Therefore, the q-binomial coefficients are polynomials in q with integer coefficients. Consider next the two sides of Equation (3.2.2) when q is transcendental. The two sides are polynomials in q, and equal when q is a prime power. Therefore, Equation (3.2.2) holds when q is transcendental. It follows similarly that Equation (3.2.3) holds in the transcendental case.

4. Matrices with different rows.

Consider the set of all $m \times t$ matrices whose rows are non-zero and mutually distinct. Let $V := \mathbf{F}_q^m$, and denote by $\xi_1, \ldots, \xi_m$ the dual of the canonical basis of V. Then, clearly, the latter set of matrices can be identified with the set of linear maps $\mathrm{Hom}_{\mathscr{D}}(\mathbf{F}_q^t, V)$ defined by the following family $\mathscr{D}$ of subspaces of V: A subspace U belongs to $\mathscr{D}$, if and only if the functionals ξ_i when restricted to U are non-zero and mutually distinct.

Clearly, the number of matrices in $\mathrm{Hom}_{\mathscr{D}}(\mathbf{F}_q^t, V)$ is $(q^t - 1)(q^t - 2)\ldots(q^t - m)$. Therefore it follows from Equation (2.2.2) that the polynomial of Corollary 2.2 is $f(x) = (x-1)(x-2)\ldots(x-m)$. Hence, from Formula (2.2.5), we obtain the following result of Carlitz [C3].

PROPOSITION 4.1. *The number $\delta_r(t,m)$ of $m \times t$ matrices of rank r with entries in $\mathbf{F}_q$, whose rows are non-zero and mutually different, is given by the following expression,*

$$\delta_r(t,m) = |\mathrm{Hom}_{\mathscr{D}_r}(\mathbf{F}_q^t, \mathbf{F}_q^m)| = \begin{bmatrix} t \\ r \end{bmatrix} \sum_{i=0}^{r} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} r \\ i \end{bmatrix} (q^{r-i} - 1)(q^{r-i} - 2)\ldots(q^{r-i} - m).$$

NOTE 4.2. The interest in the numbers $\delta_r(t,m)$ originally comes from their applications to coding theory. They appear in the investigations of the distribution of *multigrams* in solutions of maximal length of linear recurring sequences associated to linear codes. For more details see §7–10 of [Ls].

5. Matrices with quadratic symmetric conditions on the entries.

In this section the prime power q will be assumed to be odd. Let S be a regular symmetric bilinear form on V. In a given basis of V, identify S with a regular symmetric $m \times m$ matrix S. Consider the set of all $m \times t$ matrices X such that

$$X'SX = 0.$$

Clearly, the latter set of matrices can be identified with the set $\mathrm{Hom}_{\mathscr{S}}(\mathsf{F}_q^t, V)$ of linear maps defined by the set $\mathscr{S}$ of subspaces of V that are isotropic for S. Recall that a subspce $U \subseteq V$ is said to be *isotropic* for the bilinear form S if S is equal to zero on U.

5.1. Define for $\varepsilon = \pm 1$ a function $\sigma_r^{\varepsilon}(m)$ as follows: If m is odd, ignore the argument ε, and set

$$\sigma_r(m) := \prod_{i=1}^{r} \frac{q^{m+1-2i} - 1}{q^i - 1} = \prod_{i=1}^{r} \frac{(q^{\frac{m+1}{2}-i} + 1)(q^{\frac{m+1}{2}-i} - 1)}{q^i - 1}.$$

If m is even, set

$$\sigma_r^{\varepsilon}(m) := \prod_{i=1}^{r} \frac{q^{m+1-2i} + \varepsilon(q-1)q^{\frac{m}{2}-i} - 1}{q^i - 1}$$

$$= \prod_{i=1}^{r} \frac{(q^{\frac{m}{2}-i+1} - \varepsilon)(q^{\frac{m}{2}-i} + \varepsilon)}{q^i - 1} = \frac{q^{\frac{m}{2}-r} + \varepsilon}{q^{\frac{m}{2}} + \varepsilon} \prod_{i=1}^{r} \frac{q^{m+2-2i} - 1}{q^i - 1}$$

(where the last equation assumes $m > 0$ or $\varepsilon \neq -1$). Note that the numerator in the above products contains 0 as a factor when r is large. More precisely,

$$\sigma_r^{\varepsilon}(m) = 0 \Leftrightarrow \begin{cases} r > \dfrac{m-1}{2} & \text{when } m \text{ is odd,} \\ r > \dfrac{m}{2} & \text{when } m \text{ is even and } \varepsilon = 1. \\ r > \dfrac{m}{2} - 1 & \text{when } m \text{ is even and } \varepsilon = -1. \end{cases}$$

LEMMA 5.2. *Let S be a regular symmetric form on V. If the dimension m of V is*

even, define $\varepsilon = \varepsilon(S)$ *as* $+1$ *or* -1 *according as* $(-1)^{\frac{m}{2}} \det S$ *is a square or a non-square in* $\mathbf{F}_q^*$. *Then, the number of isotropic subspaces of dimension* r *for the form* S *is equal to the following expression,*

$$|\mathscr{S}_r| = \sigma_r^\varepsilon(m).$$

PROOF. The starting point of the proof is the following well known formula for the number of solutions in V to the equation $S(x, x) = 0$. The number of solutions is equal to q^{m-1} if m is odd, and equal to $q^{m-1} + \varepsilon(q-1)q^{\frac{m}{2}-1}$ if m is even, see [D, Theorems 65 and 66, pp. 47–48]. Hence the number of non-zero solutions to $S(x, x) = 0$ is equal to the expression,

$$\sigma_1^\varepsilon(m)(q-1) = \begin{cases} q^{m-1} - 1 & \text{when } m \text{ is odd,} \\ q^{m-1} + \varepsilon(q-1)q^{\frac{m}{2}-1} - 1 & \text{when } m \text{ is even.} \end{cases} \tag{5.2.1}$$

The number $|\mathscr{S}_1|$ of dimension-1 isotropic subspaces is obtained by dividing the latter expression by $q - 1$. Therefore, the formula of the Lemma holds for $r = 1$. Clearly, the formula holds for $r = 0$. In particular, the formula holds for $m = 1$ and $m = 2$. The formula is proved in the general case by induction on m.

Assume that $m > 2$. Then there are 1-dimensional isotropic subspaces of V, because the expression (5.2.1) is positive. Fix a 1-dimensional isotropic subspace L of V, and consider its "orthogonal complement" $L^\perp$. If v is a generator of L, then $L^\perp$ is the set of all vectors u such that $S(u, v) = 0$. The complement $L^\perp$ is of dimension $m - 1$, because S is regular. Moreover, $L^\perp$ contains L, because L is isotropic. The restriction, $S^\perp$, of S to $L^\perp$ is not regular, since L is contained in the null space of $S^\perp$. However, consider the form S_0 induced by $S^\perp$ on the quotient $V_0 := L^\perp/L$. Then, as will now be shown, the form S_0 is regular; moreover, $\dim V_0 = m - 2$ and, if m is even, then $\varepsilon(S) = \varepsilon(S_0)$.

To prove the latter assertions, choose a generator v for L, extend the vector v to a basis $(v, u_1, \ldots, u_{m-2})$ for $L^\perp$, and extend the latter set with a vector w to a basis $(v, w, u_1, \ldots, u_{m-2})$ for V. In the latter basis, the form S corresponds to a matrix of the following form,

$$\begin{pmatrix} 0 & a & 0 & \ldots & 0 \\ a & & & \ldots & \\ 0 & & & & \\ \vdots & \vdots & & S_0 & \\ 0 & & & & \end{pmatrix}$$

where $a = S(v, w)$ and S_0 is an $(m-2) \times (m-2)$ matrix. By Laplace development of the determinant of S we have that $\det S = -a^2 \det S_0$. The matrix S_0 is a matrix of the form S_0 defined above. Therefore, the form S_0 is regular and, for m even, $\varepsilon(S) = \varepsilon(S_0)$. Hence the assertions hold.

Consider the set of all isotropic subspaces containing L. Clearly, every isotropic subspace containing L is contained in $L^{\perp}$. Therefore, the isotropic subspaces containing L correspond bijectively to the isotropic subspaces in V_0 for the form S_0. Hence, by the induction hypothesis, the number of isotropic dimension-r subspaces containing L is equal to $\sigma^{\varepsilon}_{r-1}(m-2)$. In particular, the number is independent of L. Therefore, for $r \geqq 1$, the number $|\mathscr{S}_r|$ of all isotropic dimension-r subspaces is equal to $\sigma^{\varepsilon}_{r-1}(m-2)$ multiplied by the number $\sigma^{\varepsilon}_1(m)$ of L's and divided by the number $(q^r-1)/(q-1)$ of L's contained in a dimension-r subspace. Hence we obtain the equation,

$$|\mathscr{S}_r| = \frac{\sigma^{\varepsilon}_1(m)(q-1)}{q^r-1} \cdot \sigma^{\varepsilon}_{r-1}(m-2).$$

The numerator of the fraction is equal to the expression (5.2.1). The asserted formula follows from the definition of $\sigma^{\varepsilon}_r(m)$.

From Lemma 5.2 and Formula (2.1.1), we obtain the following result.

PROPOSITION 5.3. *Consider the $m \times t$ matrix solutions X to the equation,*

$$X'SX = 0.$$

The number $\sigma_r(t,m)$ of rank-r solutions is given by the expression,

$$\sigma_r(t,m) = |\mathrm{Hom}_{\mathscr{S}_r}(\mathsf{F}_q^t, \mathsf{F}_q^m)| = \sigma^{\varepsilon}_r(m) Q_r(q^t), \tag{5.3.1}$$

and the total number $\sigma(t,m)$ of solutions is given by the expression,

$$\sigma(t,m) = |\mathrm{Hom}_{\mathscr{S}}(\mathsf{F}_q^t, \mathsf{F}_q^m)| = \sum_r \sigma^{\varepsilon}_r(m) Q_r(q^t) \tag{5.3.2}$$

where the summation is from $r = 0$ to the upper limit given by the inequalities following the definition of σ in 5.1.

EXAMPLE 5.4. The determinant of the form S is well defined modulo the subgroup of squares, $(\mathsf{F}_q^*)^2$. If $m \equiv 0 \pmod 4$, then $\varepsilon(S) = 1$ if and only if $\det S \in (\mathsf{F}_q^*)^2$; if $m \equiv 2 \pmod 4$, then $\varepsilon(S) = 1$ if and only if $-\det S \in (\mathsf{F}_q^*)^2$. For small values of m we obtain the following expressions for $\sigma(t,m)$:

$$\sigma(t,1),$$

$$\sigma(t,2) = \begin{cases} 1 & \text{if} \quad -\det S \notin (\mathsf{F}_q^*)^2, \\ 1 + 2(q^t-1) & \text{if} \quad -\det S \in (\mathsf{F}_q^*)^2, \end{cases}$$

$$\sigma(t,3) = 1 + (q+1)(q^t-1),$$

$$\sigma(t,4) = 1 + (q^2+1)(q^t-1) \quad \text{if} \quad \det S \notin (\mathsf{F}_q^*)^2.$$

Finally, when $m = 4$ and $\det S \in (\mathsf{F}_q^*)^2$,

$$\sigma(t,4) = 1 + (q+1)^2(q^t-1) + 2(q+1)(q^t-1)(q^t-q).$$

NOTE 5.5. The expression for the number $\sigma_r(t,m)$ in (5.3.1) seems to be new. The number $\sigma(t,m)$ in (5.3.2) was considered by Carlitz [C1, Theorem 4, p. 131], who obtained a different expression. The result of Carlitz is the following: The product $q^{\frac{1}{2}t(t+1)-mt}\sigma(t,m)$ is equal to the following expression when m is odd:

$$1 + \sum_{1<2r\leqq t} q^{-(m+1)r} \frac{\prod_{i=0}^{2r-1}(1-q^{t-i})}{\prod_{i=1}^{r}(1-q^{-2i})},$$

and equal to the following expression when m is even:

$$1 + \sum_{1<2r\leqq t} q^{-mr} \frac{\prod_{i=0}^{2r-1}(1-q^{t-i})}{\prod_{i=1}^{r}(1-q^{-2i})} - \varepsilon q^{\frac{1}{2}m} \sum_{1<2r\leqq t+1} q^{-mr} \frac{\prod_{i=0}^{2r-2}(1-q^{t-i})}{\prod_{i=1}^{r-1}(1-q^{-2i})}.$$

Comparing the expressions (5.3.2) with the expressions of Carlitz we obtain a q-identity for each $m = 1, 2, \ldots$. The expressions of Carlitz can be interpreted as special values of certain generalized hypergeometric series, see [C1]. The identity obtained for $m = 1$ was observed by Carlitz [C1, Formula (4.9), p. 129]. It is the following:

$$q^{\frac{1}{2}m(m+1)} = \sum_{0\leqq 2r\leqq m+1} q^{-2r} \frac{\prod_{i=0}^{2r-1}(1-q^{m+1-i})}{\prod_{i=1}^{r}(1-q^{-2i})}.$$

6. Matrices with quadratic alternating conditions on the entries.

Let again q be an arbitrary prime power. Assume that the dimension m of V is even. Let A be a regular alternating bilinear form on V. In a given basis of V, identify A with a regular alternating $m \times m$ matrix A. Consider the set of all $m \times t$ matrices X such that

$$X'AX = 0.$$

Clearly, the latter set of matrices can be identified with the set of linear maps $\mathrm{Hom}_{\mathscr{A}}(\mathsf{F}_q^t, V)$ defined by the set $\mathscr{A}$ of subspaces of V that are isotropic for A. Recall that a subspace $U \subseteq V$ is said to be *isotropic* for the bilinear form A if A is equal to zero on U. It is easy to determine the number $|\mathscr{A}_r|$ of isotropic dimension-r subspaces. Indeed, consider a basis $(v_1, \ldots, v_i)$ for an i-dimensional isotropic subspace U. Let v be an arbitrary vector. Then $(v_1, \ldots, v_i, v)$ is a basis for an $(i+1)$-dimensional isotropic subspace, if and only if $v \notin U$ and $v \in U^\perp$. The complement $U^\perp$ has dimension $m - i$ because A is regular and $U \subseteq U^\perp$ because A is alternating. Hence the number of possible v's is equal to $q^{m-i} - q^i$. It follows by induction that the number of bases of isotropic dimension-r subspaces is equal to the product,

$$(q^m - 1)(q^{m-1} - q)(q^{m-2} - q^2)\dots(q^{m-r+1} - q^{r-1}).$$

Hence, the number of isotropic dimension-r subspaces is equal to the latter product divided by the number of bases for an r-dimensional subspace, that is, divided by $Q_r(q^r)$. Thus the number of isotropic dimension-r subspaces of V is equal to

$$\alpha_r(m) = \prod_{i=1}^{r} \frac{q^{m+2-2i} - 1}{q^i - 1}.$$

Therefore, from Formula (2.1.1) we obtain the following result.

PROPOSITION 6.1. *Consider the $m \times t$ matrix solutions X to the equation,*

$$X'AX = 0.$$

The number $\alpha_r(t, m)$ of rank-r solutions X is given by the expression,

$$\alpha_r(t, m) = |\mathrm{Hom}_{\mathscr{A}_r}(\mathbf{F}_q^t, V)| = \prod_{i=1}^{r} \frac{q^{m+2-2i} - 1}{q^i - 1} Q_r(q^t), \tag{6.1.1}$$

and the total number $\alpha(t, m)$ of solutions is given by the expression,

$$\alpha(t, m) = |\mathrm{Hom}_{\mathscr{A}}(\mathbf{F}_q^t, V)| = \sum_{r=0}^{m/2} \prod_{i=1}^{r} \frac{q^{m+2-2i} - 1}{q^i - 1} Q_r(q^t). \tag{6.1.2}$$

NOTE 6.2. It follows from the expressions for the number $\alpha_r(m)$ above and the number $\sigma_r(m)$ in Section 5 that the following equation holds,

$$\alpha_r(m) = \sigma_r(m + 1).$$

The latter equation has the following interpretation that seems to the authors to be a strange coincidence. Work over a finite field with an odd number q of elements. Assume that m is even. Let A be an alternating regular $m \times m$ matrix and let S be a symmetric regular $(m + 1) \times (m + 1)$ matrix. Then the number of dimension-r isotropic subspaces for A is equal to the number of dimension-r isotropic subspaces for S.

NOTE 6.3. An alternative expression for the number $\alpha(t, m)$ in (6.1.2) was obtained by Carlitz in [C2, Theorem 4, p. 25] using exponential sums. The result of Carlitz is the following:

$$q^{\frac{1}{2}t(t-1)}\alpha(t, m) = \sum_{0 \le 2r \le t} q^{m(t-r)-2r} \frac{\prod_{i=0}^{2r-1}(1 - q^{t-i})}{\prod_{i=1}^{r}(1 - q^{-2i})}.$$

In [C2], the exponent of q in the first term in the sum was erroneously given as $m(2t - r) - 2r$.

As in Section 5, the expressions of Carlitz can be interpreted as special values of

b⇒
hypergeometric series. Comparing the expression of Carlitz with the expression (6.1.2) we obtain for an even integer m the following q-identity:

$$\sum_{0 \leqq 2r \leqq t} q^{m(t-r)-2r} \frac{\prod_{i=0}^{2r-1}(1-q^{t-i})}{\prod_{i=1}^{r}(1-q^{-2i})} = q^{\frac{1}{2}t(t-1)} \sum_{r=0}^{m/2} \prod_{i=1}^{r} \frac{(q^{m+2-2i}-1)(q^t-q^{i-1})}{q^i-1}.$$

7. Recursion formulas.

In this section we return to the setup of Section 1. We prove a recursion formula for the coefficients in the interpolation formulas. When applied to the sequence $\lambda_i := q^{i-1}$, we recover the recursion formulas for the numbers $\phi_r(t,m)$ and $\delta_r(t,m)$ considered in Sections 4 and 5.

LEMMA 7.1. *The polynomial $f(x)$ can be factored in $R[x]$ as $f(x) = (x-\lambda)g(x)$ if and only if the recursion formulas,*

$$\begin{bmatrix} f \\ r \end{bmatrix} = (\lambda_{r+1} - \lambda)\begin{bmatrix} g \\ r \end{bmatrix} + \begin{bmatrix} g \\ r-1 \end{bmatrix},$$

or equivalently, the formulas

$$\begin{bmatrix} f \\ r \end{bmatrix} Q_r(x) = (\lambda_{r+1} - \lambda)\begin{bmatrix} g \\ r \end{bmatrix} Q_r(x) + (x-\lambda_r)\begin{bmatrix} g \\ r-1 \end{bmatrix} Q_{r-1}(x),$$

hold for $r = 1, 2, \ldots$.

PROOF. All the assertions of the Lemma follow immediately from the formulas

$$(x-\lambda)Q_r(x) = (\lambda_{r+1} - \lambda)Q_r(x) + Q_{r+1}(x) \quad \text{for} \quad r = 0, 1, \ldots.$$

7.2. As we saw in Section 3 and 4, the two conditions (1) and (2) considered in the Introduction correspond to the numbers $\phi_r(t,m)$ and $\delta_r(t,m)$ defined in Proposition 3.1 and Proposition 4.1. By Formula (2.2.4) and Note 3.2,

$$\phi_r(t,m) = \begin{bmatrix} f_m \\ r \end{bmatrix} Q_r(q^t),$$

where $f_m = x^m$. Hence, by applying Lemma 7.1 to the factorization $f_m(x) = xf_{m-1}(x)$, we obtain the following recursion formulas of Landsberg [Lb],

$$\phi_r(t,m) = q^r\phi_r(t,m-1) + (q^t - q^{r-1})\phi_{r-1}(t,m-1).$$

Similarly, by formula (2.2.4) and the analysis of Section 4,

$$\delta_r(t,m) = \begin{bmatrix} f_m \\ r \end{bmatrix} Q_r(q^t)$$

where $f_m(x) = (x-1)(x-2)\ldots(x-m)$. Here $f_m(x) = (x-m)f_{m-1}(x)$, and we obtain the recursion formulas of Laksov [Ls],

$$\delta_r(t,m) = (q^r - m)\delta_r(t,m-1) + (q^t - q^{r-1})\delta_{r-1}(t,m-1).$$

REFERENCES

[C1] L. Carlitz, *Representations by quadratic forms in a finite field*, Duke. Math. J. 21 (1954), 123–138.

[C2] L. Carlitz, *Representations by skew forms in a finite field*, Arch. Math. 5 (1954), 19–31.

[C3] L. Carlitz, *Note on a paper of Laksov*, Math. Scand. 19 (1966), 38–40.

[D] L. E. Dickson, *Linear Groups*, Teubner, Leipzig, 1901.

[H1] J. H. Hodges, *Representations by bilinear forms in a finite field*, Duke Math. J. 22 (1955), 497–510.

[H2] J. H. Hodges, *Exponential sums for skew matrices in a finite field*, Arch. Math. 7 (1956), 116–121.

[H3] J. H. Hodges, *Some matrix equations in a finite field*, Annali di Matematica 44 (1957), 245–250.

[H4] J. H. Hodges, *A bilinear matrix equation over a finite field*, Duke Math. J. 31 (1964), 661–666.

[H5] J. H. Hodges, *A skew matrix equation over a finite field*, Arch. Math. 17 (1966), 49–55.

[Ls] D. Laksov, *Linear recurring sequences over finite fields*, Math. Scand. 16 (1965), 181–196.

[Lb] G. Landsberg, *Über eine Anzahlbestimmung und eine damit zusammenhängende Reihe*, J. Reine Angew. Math. 111 (1893), 87–88.

[P] A. D. Porter, *Some partitions of a skew matrix*, Ann. Mat. Pura Appl. 82 (1969), 115–120.

[P-M1] A. D. Porter and N. Mousouris, *Ranked solutions of some matrix equations*, Linear and Multilinear Algebra 6 (1978), 145–151.

[P-M2] A. D. Porter and N. Mousouris, *Exponential sums and rectangular partitions*, Linear Algebra Appl. 29 (1980), 347–355.

[P-M3] A. D. Porter and N. Mousouris, *Ranked symmetric matrix equations*, Algebras Groups Geom. 4 (1987), 383–394.

[P-R] A. D. Porter and A. A. Riveland, *A generalized skew equation over a finite field*, Math. Nachr. 69 (1975), 291–296.

MATEMATISKA INSTITUTIONEN
KTH
S-100 44 STOCKHOLM
SWEDEN

MATEMATISK INSTITUT
UNIVERSITETSPARKEN 5
DK-2100 KØBENHAVN Ø
DENMARK