Pacific Journal of Mathematics

THE NUMBER OF SOLUTIONS OF SOME SPECIAL EQUATIONS IN A FINITE FIELD

L. CARLITZ

Vol. 4, No. 2 June 1954

THE NUMBER OF SOLUTIONS OF SOME SPECIAL EQUATIONS IN A FINITE FIELD

L. CARLITZ

1. Introduction. Let $GF(q)$ denote a fixed finite field. If

$$f(x) = f(x_1, \cdots, x_r)$$

is a polynomial with coefficients in $GF(q)$, and $\alpha \in GF(q)$, let

$$N_f(\alpha) = N\{f(\xi_1, \cdots, \xi_r) = \alpha,\ \xi_i \in GF(q)\}$$

denote the number of solutions of the equation $f(\xi) = \alpha$. For certain polynomials f we have

$$N_f(\alpha) = N_f(1) \qquad (\alpha \neq 0); \tag{1.1}$$

that is, $N_f(\alpha)$ is fixed for all $\alpha \neq 0$. For example, if q is odd and

$$f(x) = Q(x_1, \cdots, x_r),$$

a quadratic form of discriminant $\delta \neq 0$ and $r = 2s$, then as is well known

$$N_Q(\alpha) = q^{2s-1} + q^{s-1} k(\alpha)\psi((-1)^s \delta), \tag{1.2}$$

where

$$k(\alpha) = \begin{cases} q-1 & (\alpha = 0) \\ -1 & (\alpha \neq 0), \end{cases} \tag{1.3}$$

and $\psi(\alpha) = 0, +1, -1$ according as $\alpha = 0$, a square or a nonsquare of $GF(q)$ Another example of (1.1) is furnished by the polynomial [2, Theorem 4]

$$g(x) = \sum_{i=1}^{s} \alpha_i \prod_{j=1}^{r_i} x_{ij}^{a_{ij}} = \alpha \qquad (\alpha_i \neq 0) \tag{1.4}$$

Received March 17, 1953.

Pacific J. Math. 4 (1954), 207-217

where the exponents a_{ij} satisfy

$$(a_{i1}, \cdots, a_{ir_i}) = 1 \qquad (i = 1, \cdots, s).$$

We now have

$$(1.5) \qquad N_g(\alpha) = q^{r-1} + q^{-1} k(\alpha) \prod_{i=1}^{s} (q^{r_i} - q(q-1)^{r_i-1}),$$

where $r = r_1 + r_2 + \cdots + r_s$.

An instance of a somewhat different kind is furnished by $\Delta(x) = |x_{ij}|$, the determinant of order x in the r^2 indeterminates x_{ij}. The number of solutions of $\Delta(\xi) = \alpha$ is given by [5]

$$(1.6) \qquad N_\Delta(\alpha) = q^{r^2-1} + k(\alpha)\left\{q^{r^2-1} - q^{\frac{1}{2}r(r-1)} \prod_{2}^{r} (q^i - 1)\right\},$$

where again $k(\alpha)$ is defined by (1.3). We shall show below that if $P(x)$ denotes the Pfaffian in the $r(2r-1)$ indeterminates x_{ij}, $1 \leq i < j \leq 2r$, then

$$(1.7) \qquad N_P(\alpha) = q^{(r-1)(2r+1)} + k(\alpha)\left\{q^{(r-1)(2r+1)} - q^{r(r-1)} \prod_{i=1}^{r-1} (q^{2i+1} - 1)\right\};$$

in particular,

$$(1.8) \qquad N_P(1) = q^{r(r-1)} (q^3 - 1)(q^5 - 1) \cdots (q^{2r-1} - 1).$$

The result (1.7) may of course be expressed in terms of $N_S(\alpha)$, where $S(x)$ is the general skew-symmetric determinant of even order. The corresponding result for symmetric determinants seems more difficult to obtain and will not be discussed in the present note.

Returning to (1.1), we note that it is easy to show that if the polynomials f and g satisfy (1.1) then the same is true of

$$h(x, y) = f(x) + g(y),$$

where the x's and y's are distinct. More precisely, if

$$N_f(\alpha) = A + k(\alpha)B, \qquad N_g(\alpha) = C + k(\alpha)D,$$

then

$$N_h(\alpha) = q\{AC + k(\alpha)BD\}. \tag{1.9}$$

By means of (1.9) and the other formulas stated above we may derive many additional instances of (1.1). To mention one example,

$$\begin{aligned} N\{P_1(x^{(1)}) + \cdots + P_s(x^{(s)}) = \alpha\} &= q^{(r-1)(2r+1)s+s-1} \\ &\quad + k(\alpha)q^{s-1}\left\{q^{(r-1)(2r+1)} - q^{r(r-1)}\prod_{i=1}^{r-1}(q^{2i+1} - 1)\right\}^s, \end{aligned} \tag{1.10}$$

where each of the Pfaffians P_i contain $r(2r-1)$ unknowns; the total number of unknowns is $rs(2r-1)$. We can also determine the number of solutions of the equation $S(\xi) + S'(\eta) = \alpha$, where S and S' denote skew-symmetric determinants, but the result is rather complicated. For a more general result of this kind see Theorem 5 below.

Finally we determine the number of solutions of

$$F_1(x^{(1)}) + \cdots + F_s(x^{(s)}) = \alpha,$$

where each F is homogeneous and irreducible and factors completely into linear factors in some extended field $GF(q^m)$.

2. Pfaffians.

For properties of the Pfaffian

$$P(x_{12}, \cdots, x_{2r-1,2r}) = (1, 2, 3, \cdots, 2r)$$

see for example [6, §61]. We recall in particular the recursion formula

$$\begin{aligned} (1, 2, 3, \cdots, 2r) &= x_{12}(3, 4, \cdots, 2r) + x_{13}(4, 5, \cdots, 2r, 2) \\ &\quad + \cdots + x_{1,2r}(2, 3, \cdots, 2r-1). \end{aligned} \tag{2.1}$$

Now consider the equation

$$P(x) = \alpha \qquad (\alpha \neq 0). \tag{2.2}$$

Since, by (2.1), P is linear and homogeneous in $x_{12}, x_{13}, \cdots, x_{1,2r-1}$, it is clear that P satisfies (1.1). To determine $N_P(1)$, we consider the general skew-symmetric determinant of even order

$$(2.3) \qquad S(x) = |x_{ij}| \qquad (i, j = 1, \cdots, 2r;\ x_{ij} = -x_{ji})$$

and the bilinear form

$$B(u, v) = \sum_{i,j=1}^{2r} x_{ij} u_i v_j .$$

It is familiar that, by applying the same nonsingular linear transformation to the u's and v's, $B(u, v)$ can be reduced to normal form with matrix

$$(2.4) \qquad \begin{pmatrix} E_1 & & & & \\ & E_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & E_r \end{pmatrix}, \qquad E_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now on the other hand a bilinear form with matrix (2.5) is invariant under a group of order [4, § 115]

$$q^{r^2}(q^2-1)(q^4-1)\cdots(q^{2r}-1).$$

Since the total number of nonsingular matrices of order $2r$ is equal to

$$q^{r(2r-1)}(q-1)(q^2-1)(q^3-1)\cdots(q^{2r}-1),$$

it follows that the number of skew-symmetric determinants $S(x) = \alpha^2$ is determined by

$$2q^{r(r-1)}(q^3-1)(q^5-1)\cdots(q^{2r-1}-1).$$

Finally since $S(x) = P^2(x)$ it follows that

$$(2.5) \qquad N_P(\alpha) = q^{r(r-1)} \prod_{i=2}^{r} (q^{2i-1}-1) \qquad (\alpha \neq 0).$$

Since

$$N_P(0) + (q-1)N_P(1) = q^{r(2r-1)},$$

we get also

$$N_P(0) = q^{r(2r-1)} - q^{r(r-1)} \prod_{i=1}^{r} (q^{2i-1} - 1). \tag{2.6}$$

We may now state:

THEOREM 1 (q odd). *If $P(x)$ denotes the general Pfaffian in $r(2r-1)$ indeterminates, then the number of solutions of the equation $P(\xi) = \alpha$ is furnished by* (2.5) *and* (2.6).

It is easily verified that (2.5) and (2.6) imply (1.7).

As for $S(x)$ we have:

THEOREM 2 (q odd). *If $S(x)$ denotes the general skew-symmetric determinant of order $2r$, then*

$$N_S(\alpha) = (1 + \psi(\alpha))N_P(\alpha), \tag{2.7}$$

where $\psi(\alpha) = 0, +1, -1$ according as $\alpha = 0$, a square or a nonsquare of $GF(q)$.

3. Some general results. If the polynomial $f(x)$ is such that

$$N_f(0) = l_0, \qquad N_f(\alpha) = l_1 \qquad (\alpha \neq 0), \tag{3.1}$$

then it is easily verified that

$$N_f(\alpha) = A + k(\alpha)B, \tag{3.2}$$

where $k(\alpha)$ is defined by (1.3) and

$$qA = l_0 + (q-1)l_1, \quad qB = l_0 - l_1. \tag{3.3}$$

Conversely (3.2) and (3.3) imply (3.1). (Compare [**1**, § 9].)

We now prove:

THEOREM 3. *The function $k(\alpha)$ satisfies*

$$\sum_{\xi+\eta=\alpha} k(\xi) = 0, \qquad \sum_{\xi+\eta=\alpha} k(\xi)k(\eta) = qk(\alpha). \tag{3.4}$$

The first equality follows from

$$\sum_{\xi+\eta=\alpha} k(\xi) = \sum_{\xi} k(\alpha) = k(0) + (q-1)k(1) = 0.$$

To prove the second, we have first, for $\alpha = 0$,

$$\sum_{\xi+\eta=0} k(\xi)k(\eta) = \sum_{\xi} k^2(\xi) = (q-1)^2 + (q-1) = q(q-1),$$

while for $\alpha \neq 0$,

$$\sum_{\xi+\eta=\alpha} k(\xi)k(\eta) = k(\alpha)k(0) + k(0)k(\alpha) + \sum_{\xi \neq 0,\alpha} k(\xi)k(\alpha-\xi)$$

$$= -2(q-1) + (q-2) = q.$$

This evidently completes the proof of (3.4).

If we define the dot product of two functions k_1, k_2 by means of

$$(3.5) \qquad k_1 \cdot k_2(\alpha) = \sum_{\xi+\eta=\alpha} k_1(\xi)k_2(\eta),$$

then (3.4) can be written as

$$(3.6) \qquad 1 \cdot k = 0, \qquad k \cdot k = qk,$$

where the function 1 is defined by $1(\alpha) = 1$ for all α. The product is associative and commutative.

Returning to (3.2), let f and g be polynomials such that

$$(3.7) \qquad N_f(\alpha) = A + k(\alpha)B, \qquad N_g(\alpha) = C + k(\alpha)D.$$

Also let

$$(3.8) \qquad h(x, y) = f(x_1, \cdots, x_r) + g(y_1, \cdots, y_s),$$

where the x's and y's are distinct indeterminates. We prove that

$$(3.9) \qquad N_h(\alpha) = q\{AC + k(\alpha)BD\}.$$

Clearly we have

$$N_h(\alpha) = \sum_{\beta+\gamma=\alpha} N_f(\beta) N_g(\gamma) = \sum_{\beta+\gamma=\alpha} (A + k(\beta)B)(C + k(\gamma)D)$$

$$= q\{AC + k(\alpha)BD\}$$

by (3.4). We now state:

THEOREM 4. *If the polynomials f, g satisfy* (3.7), *and h is defined by* (3.8), *then* $N_h(\alpha)$ *is determined by* (3.9).

In terms of (3.5) we may state that the functions of the form (3.2) are closed with respect to dot multiplication. (Compare [**3**, § 3].)

As an immediate corollary of Theorem 4 we see that if

$$h(x^{(1)}, \cdots, x^{(s)}) = \alpha_1 f(x^{(1)}) + \cdots + \alpha_s f(x^{(s)}) \qquad (\alpha_i \neq 0),$$

where f satisfies (3.2), then

$$N_h(\alpha) = q^{s-1}(A^s + k(\alpha)B^s). \tag{3.10}$$

Applying (3.10) to Theorem 1 we immediately get (1.10). Similarly if we apply (3.10) to (1.6) and put

$$h(x) = |x_{ij}^{(1)}| + \cdots + |x_{ij}^{(s)}|, \tag{3.11}$$

we get the result

$$N_h(\alpha) = q^{r^2 s-1} + q^{s-1}k(\alpha)\left\{q^{r^2-1} - q^{\frac{1}{2}r(r-1)} \prod_2^r (q^i - 1)\right\}^s. \tag{3.12}$$

It is of course not necessary that the determinants in the right member of (3.11) be of the same order.

Additional results like (3.12) as well as various mixed results using (1.2), (1.5), (1.6), and (1.7) are readily obtained.

4. Another theorem. In view of (2.7) we consider functions of the form

$$j(\alpha) = (1 + \psi(\alpha))l(\alpha), \tag{4.1}$$

where as in (3.1) $l(0)=l_0$, $l(\alpha)=l_1$ for $\alpha \neq 0$. If $j'(\alpha)=(1+\psi(\alpha))l'(\alpha)$, $l'(0)=l_0'$, $l'(\alpha)=l_1'$ for $\alpha \neq 0$, is a second function of the same kind, we may compute

$$S = \sum_{\xi+\gamma=\alpha} j(\xi)j'(\eta). \tag{4.2}$$

Indeed, for $\alpha=0$,

$$S = l(0)l(0) + \sum_{\xi\neq 0} (1+\psi(\xi))(1+\psi(-\xi))l(\xi)l'(-\xi)$$

$$= l_0l_0' - l_1l_1' + l_1l_1' \sum_{\xi} (1+\psi(\xi))(1+\psi(-\xi)),$$

while for $\alpha \neq 0$,

$$S = (1+\psi(\alpha))(l(0)l'(\alpha)+l(\alpha)l'(0))$$

$$+ \sum_{\xi\eta\neq 0} (1+\psi(\xi))(1+\psi(\eta))l(\xi)l'(\eta).$$

$$= (1+\psi(\alpha))(l_0l_1' + l_0'l_1 - 2l_1l_1') + l_1l_1' \sum_{\xi+\eta=\alpha} (1+\psi(\xi))(1+\psi(\eta)).$$

But by (1.2),

$$\sum_{\xi+\eta=\alpha} (1+\psi(\xi))(1+\psi(\eta)) = q + k(\alpha)\psi(-1).$$

Hence we get:

THEOREM 5. *The sum* (4.2) *is evaluated by means of*

$$S = (1+\psi(\alpha))l''(\alpha) + l_1l_1'\{q + k(\alpha)\psi(-1)\}, \tag{4.3}$$

where

$$l''(0) = l_0l_0' - l_1l_1', \quad l''(\alpha) = l_0l_1' + l_0'l_1 - 2l_1l_1' \qquad (\alpha \neq 0).$$

Note that the right member of (4.3) is the sum of a function of the type (4.1) and one of the type (3.1).

If we identify (4.1) with (2.7) we get the number of solutions of the equation

$$S(\xi) + S'(\eta) = \alpha, \tag{4.4}$$

where S and S' denote skew-symmetric determinants in ξ_{ij}, η_{ij} respectively. It seems unnecessary to state the final formulas which are somewhat complicated.

By means of Theorem 5 we may also obtain the number of solutions of such equations as

$$\beta Q^2(x) + \gamma Q'^2(y) = \alpha \qquad (\beta\gamma \neq 0), \tag{4.5}$$

where Q, Q' denote quadratic forms in an even number of unknowns.

As for the equation

$$\Delta(x) + S(y) = \alpha, \tag{4.6}$$

where Δ is a general determinant and S is skew-symmetric, the situtation is somewhat simpler. It is now necessary to evaluate

$$\sum_{\xi+\eta=\alpha} (1 + \psi(\eta)) l(\xi) l'(\eta). \tag{4.7}$$

By means of a straightforward computation we find that (4.7) reduces to

$$\begin{cases} l_0 l_0' + (q-1) l_1 l_1' & (\alpha = 0) \\ (l_0 l_1' - l_1 l_1')(1 + \psi(\alpha)) + l_1 (l_0' + (q-1) l_1') & (\alpha \neq 0). \end{cases} \tag{4.8}$$

In particular, substituting from (1.2) and (2.7) in (4.8), we get the number of solutions of (4.6).

5. Factorable polynomials. Let $F(x) = F(x_1, \cdots, x_r)$ denote a homogeneous polynomial of degree m that is irreducible but factors completely over $GF(q^r)$. An example of such a polynomial is furnished by

$$F(x) = \prod_{i=0}^{r-1} (x_1 + \alpha^{q^i} x_2 + \cdots + \alpha^{(r-1)q^i} x_r), \tag{5.1}$$

where α is a primitive number of $GF(q^r)$. In general we may put

$$F(x) = \prod_{i=0}^{r-1} (x_1 + \alpha_2^{q^i} x_2 + \cdots + \alpha_r^{q^i} x_r), \tag{5.2}$$

where α_i is of degree f_i and r is the least common multiple of $f_2, \cdots, f_r$; we also assume that the determinant

$$|1\, \alpha_2^{q^i} \cdots \alpha_r^{q^i}| \neq 0. \qquad (i = 0, 1, \cdots, r-1).$$

It follows without difficulty that the number of solutions of $F(x) = \alpha$ is

$$N_F(\alpha) = \begin{cases} 1 & (\alpha = 0) \\ (q^r - 1)/(q-1) & (\alpha \neq 0). \end{cases} \tag{5.3}$$

We may rewrite (5.3) as

$$N_F(\alpha) = q^{r-1} - \frac{q^{r-1} - 1}{q - 1} k(\alpha). \tag{5.4}$$

Hence applying Theorem 4 we get the following result.

THEOREM 6. *Let F_i denote polynomials of the type* (5.2), deg $F_i = r_i$. *Then the number of solutions of*

$$\alpha_1 F_1(x^{(1)}) + \cdots + \alpha_s F_s(x^{(s)}) = \alpha \qquad (\alpha_i \neq 0)$$

is determined by

$$N = q^{s-1}\left\{ q^{r_1 + \cdots + r_s - s} + (-1)^s k(\alpha) \prod_{i=1}^{s} \frac{q^{r_i - 1} - 1}{q - 1} \right\}. \tag{5.5}$$

It is easily verified that for $r_i = 2$, $i = 1, \cdots, s$, (5.5) is in agreement with (1.2).

REFERENCES

1. L. Carlitz, *Invariant theory of equations in a finite field*, Trans. Amer. Math. Soc. 75 (1953), 405-427.

2. L. Carlitz, *The number of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. 38 (1952), 515-519.

3. Eckford Cohen, *Rings of arithmetic functions*, Duke Math. J. **19** (1952), 115-129.

4. L. E. Dickson, *Linear groups*, Leipzig, 1901.

5. N. J. Fine and I. Niven, *The probability that a determinant be congruent to a* (mod m), Bull. Amer. Math. Soc. 50 (1944), 89-93.

6. G. Kowalewski, *Einführung in die Determinantentheorie*, Leipzig, 1909.

DUKE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, E.G. Straus, at the University of California Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50; back numbers (Volumes 1, 2, 3) are available at $2.50 per copy. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to the publishers, University of California Press, Berkeley 4, California.

Printed at Ann Arbor, Michigan. Entered as second class matter at the Post Office, Berkeley, California.

*To be succeeded in 1955, by H.L. Royden, Stanford University, Stanford, California.

**To be succeeded in 1955, by E.G. Straus, University of California, Los Angeles 24, Calif.

UNIVERSITY OF CALIFORNIA PRESS • BERKELEY AND LOS ANGELES

Pacific Journal of Mathematics

Vol. 4, No. 2 June, 1954