A NOTE ON PARTITIONS IN $GF[q, x]$

L. CARLITZ

1. Introduction. In this note we consider problems of the following kind. For given $A \in GF[q, x]$, $A \neq 0$, let $\phi(A)$ denote the number of solutions $U_i$ of

\begin{equation}
A = U_1 + U_2 + \cdots \quad (\deg A = \deg U_1 > \deg U_2 > \cdots).
\end{equation}

Also let $\phi'(A)$ denote the number of solutions of (1.1) subject to the additional restriction that all the polynomials are primary. We may also consider various modifications of these problems; for example the degree of some or all the $U_i$ may be specified. In particular let $r(A)$ denote the number of solutions of (1.1) such that

\begin{equation}
\deg U_i = m - i + 1 \quad (i = 1, 2, \cdots, m + 1),
\end{equation}

where $m = \deg A$, and let $r'(A)$ denote the corresponding number with all $U_i$ primary. Again returning to (1.1) we may restrict the number of parts; thus let $\phi_k(A)$ denote the number of solutions of

\begin{equation}
A = U_1 + \cdots + U_k \quad (\deg U_1 > \deg U_2 > \cdots),
\end{equation}

and let $\phi_k'(A)$ denote the corresponding number when all the polynomials are primary. Other such problems are readily devised.

We find that the numbers just defined can be evaluated rather simply; thus these partition problems are considerably simpler than the corresponding problems involving integers (see for example [1, Chap. 19]). We prove the following results ($\deg A = m$):

\begin{equation}
\phi(A) = \prod_{i=0}^{m-1} (1 + (q - 1)q^i),
\end{equation}

\begin{equation}
\phi'(A) = \prod_{i=0}^{m-1} (1 + q^i),
\end{equation}

\begin{equation}
r(A) = (q - 1)^m q^{m(m-1)/2},
\end{equation}

\begin{equation}
r'(A) = q^{m(m-1)/2},
\end{equation}

\begin{equation}
\phi_k(A) = q^{(k-1)(k-2)/2}(q - 1)^k \left[ \begin{array}{c} m \\ k - 1 \end{array} \right] \quad (k \geq 1),
\end{equation}

\begin{equation}
\phi_k'(A) = q^{(k-1)(k-2)/2} \left[ \begin{array}{c} m \\ k - 1 \end{array} \right] \quad (k \geq 1),
\end{equation}

Presented to the Society, February 28, 1953; received by the editors October 27, 1952.

464
where in (1.8) and (1.9)

\[(1.10) \quad \binom{m}{k} = \frac{(q^m - 1) \cdots (q - 1)}{(q - 1) \cdots (q^k - 1)} = \binom{m}{m - k}, \quad \binom{m}{0} = 1.\]

Note that in each case the number of partitions depends only on the degree of A. It will be recalled that, if q is replaced by an indeterminate, then

\[\binom{m}{k}\]

is the generating function for partitions into at most k parts, each part being \(\leq m - k\) [2, p. 5]. We also note that (1.9) is equivalent to

\[(1 + x)(1 + qx) \cdots (1 + q^{m-1}x) = \sum_{k=0}^{m} p_k(m)x^k.\]

Similar generating functions can be constructed for the remaining partition functions.

In §5 we consider a special quadratic partition problem similar to that concerning \(r(A)\) and \(r'(A)\).

2. Proof of (1.4) and (1.5). Put

\[(2.1) \quad A = a_0x^m + a_1x^{m-1} + \cdots + a_m, \quad U_1 = b_0x^m + b_1x^{m-1} + \cdots + b_m \quad (a_i, b_i \in GF(q)).\]

Then \(b_0 = a_0\) but \(U_1\) is otherwise arbitrary. It is then clear that \(p(A)\) depends only on the degree of \(A\); we may accordingly put \(p(A) = p(m)\). Now if \(b_1 \neq a_1\), \(\deg (A - U_1) = m - 1\); otherwise \(\deg (A - U_1) < m - 1\). Thus for \(q - 1\) choices of \(b_1\) and arbitrary choice of \(b_2, \cdots, b_m\), \(\deg (A - U_1) = m - 1\). In the next place when \(b_1 = a_1\), then for \(q - 1\) choices of \(b_2\) and arbitrary choice of \(b_3, \cdots, b_m\), \(\deg (A - U_1) = m - 2\). It is clear that in this way we get the recursion

\[(2.2) \quad p(m) = (q - 1)q^{m-1}p(m - 1) + \cdots + (p - 1)q \cdot p(1) + (p - 1) \cdot p(0).\]

Clearly (2.2) implies

\[p(m) = (q - 1)q^{m-1}p(m - 1) + p(m - 1),\]

or what is the same thing

\[(2.3) \quad p(m) = (1 + (q - 1)q^{m-1})p(m - 1) \quad (m \geq 1).\]

Since \(p(0) = 1\), (1.4) follows immediately.
Next let $a_0 = b_0 = 1$. We require that all $U_i$ be primary. Thus either $a_1 - b_1 = 1$, and $b_2, \ldots, b_m$ are arbitrary, or $a_1 = b_1$. In the latter case either $a_2 - b_2 = 1$, $b_3, \ldots, b_m$ arbitrary, or $a_2 = b_2$, and so on. Thus corresponding to (2.2) we get

$$p'(m) = q^{m-1} \cdot p'(m - 1) + \cdots + q \cdot p'(1) + p'(0),$$

since again it is clear that $p'(A) = p'(m)$. It follows from (2.4) that

$$p'(m) = (1 + q^{m-1})p'(m - 1) \quad (m \geq 1).$$

Since $p'(0) = 1$, (1.5) follows at once.

3. Proof of (1.6) and (1.7). We seek $U_i$ satisfying both (1.1) and (1.2). Using the notation (2.1), again $a_0 = b_0$; however it is now necessary that $a_1 \neq b_1$. Thus there are $q - 1$ choices of $b_1$ while $b_2, \ldots, b_m$ are arbitrary. Consequently

$$r(A) = r(m) = (q - 1)q^{m-1} \cdot r(m - 1) \quad (m \geq 1).$$

Since $r(0) = 1$, we see that (3.1) implies

$$r(m) = (q - 1)^m q^{m(m-1)/2},$$

which is the same as (1.6).

As for $r'(A)$ it is clear that in place of (3.1) we get

$$r'(m) = q^{m-1} \cdot r'(m - 1) \quad (m \geq 1);$$

(1.7) is an immediate consequence of (3.2).

The definition of $r(A)$ and $r'(A)$ can be modified in various ways. For example, let $e_1, \ldots, e_k$ be fixed integers such that $m = e_1 > e_2 > \cdots > e_k \geq 0$. Then it is easily proved that the number of solutions of

$$A = U_1 + \cdots + U_k \quad \text{(deg } U_i = e_i)$$

is furnished by

$$q^{e_1 + \cdots + e_k},$$

while if $A$ is primary, then the number of primary solutions of (3.3) is

$$q^{e_1 + \cdots + e_k}.$$  

For $e_i = m - i + 1$, (3.4) and (3.5) reduce to (1.6) and (1.7) respectively.

4. Proof of (1.8) and (1.9). It is convenient to consider

$$w_k(A) = p_k(A) + \cdots + p_1(A),$$

$$w_k'(A) = p_k'(A) + \cdots + p_1'(A),$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
so that \( w_k(A), w'_k(A) \) enumerate the number of partitions of the respective kinds into at most \( k \) parts. Then as before we have

\[
(4.2) \quad w_k(m) - w_k(m - 1) = (q - 1)q^{m-1}w_{k-1}(m - 1) \quad (k \geq 2).
\]

If we introduce the generating function

\[
(4.3) \quad f_k(x) = \sum_{m=0}^{\infty} w_k(m)x^m,
\]

we find that (4.2) implies

\[
(4.4) \quad (1 - x)f_k(x) = 1 + (q - 1)xw_{k-1}(qx) \quad (k \geq 2).
\]

Since \( f_1(x) = (1-x)^{-1} \), (4.4) yields

\[
(4.5) \quad f_k(x) = \sum_{i=0}^{k-1} \frac{(q - 1)q^i(i-1)/2x^i}{(1 - x)(1 - qx) \cdots (1 - q^{k-1}x)}.
\]

Using the familiar formula

\[
\frac{1}{(1 - x)(1 - qx) \cdots (1 - q^{k-1}x)} = \sum_{m=0}^{\infty} \left[ \begin{array}{c} m + k - 1 \\ k - 1 \end{array} \right] x^m,
\]

where

\[
\left[ \begin{array}{c} m \\ k \end{array} \right]
\]

is defined by (1.10), (4.5) becomes

\[
(4.6) \quad w_k(m) = \sum_{i=0}^{k-1} (q - 1)q^i(i-1)/2 \sum_{m=0}^{\infty} \left[ \begin{array}{c} m + i \\ i \end{array} \right] x^m.
\]

Comparison with (4.3) gives

\[
(4.6) \quad w_k(m) = \sum_{i=0}^{k-1} (q - 1)q^i(i-1)/2 \left[ \begin{array}{c} m \\ i \end{array} \right].
\]

Consequently by (4.1)

\[
\hat{p}_k(m) = w_k(m) - w_{k-1}(m) = (q - 1)^{k-1}q^{(k-1)(k-2)/2} \left[ \begin{array}{c} m \\ k - 1 \end{array} \right],
\]

which proves (1.8).

The proof of (1.9) is quite similar. In place of (4.2) we now have

\[
(4.6) \quad w'_k(m) - w'_k(m - 1) = q^{m-1}w_{k-1}(m - 1) \quad (k \geq 2).
\]
Then if we put

\[ f'_k(x) = \sum_{m=0}^{\infty} w'_k(m) x^m, \]

we find that

\[(1 - x)f'_k(x) = 1 + xf_{k-1}(qx) \quad (k \geq 2), \]

whence

\[ f'_k(x) = \sum_{i=0}^{k-1} \frac{q^{(i-1)/2} x^i}{(1 - x)(1 - qx) \cdots (1 - q^i x)} \]

so that

\[(4.7) \quad w'_k(m) = \sum_{i=0}^{k-1} q^{(i-1)/2} \left[ \begin{array}{c} m \\ i \end{array} \right], \]

and therefore

\[ p'_k(m) = w'_k(m) - w'_{k-1}(m) = q^{(k-1)(k-2)/2} \left[ \begin{array}{c} m \\ k-1 \end{array} \right]. \]

Note that by definition \( w_{m+1}(m) = p(m), \ w'_{m+1}(m) = p'(m), \) and it is easy to verify that (4.6) and (4.7) reduce to (1.4) and (1.5) for \( k = m+1. \) Also by definition \( p_{m+1}(m) = r(m), \ p'_{m+1}(m) = r'(m), \) and it is evident that (1.8) and (1.9) reduce to (1.6) and (1.7) for \( k = m+1. \)

5. A quadratic problem (q odd). We now briefly consider the following special quadratic partition problem. Let \( \deg A = 2m \) and for simplicity take \( A \) primary. We seek the number of solutions in primary \( U_i \) of

\[(5.1) \quad A = U_1^2 + \cdots + U_m^2 + c \quad (\deg U_i = m - i + 1), \]

where \( c \) is some number \( \in GF(q). \) Now if we put

\[ A = x^{2m} + a_1 x^{2m-1} + \cdots + a_{2m}, \ U_1 = x^m + b_1 x^{m-1} + \cdots + b_m x^m, \]

then \( A - U_1^2 \) will be primary of degree \( 2m - 2 \) provided \( 2b_1 = a_1, \ b_1^2 + 2b_2 + 1 = a_2. \) Thus \( b_1, b_2 \) are uniquely determined while \( b_3, \ldots, b_m \) are arbitrary. If then we denote the number of solutions of (5.1) by \( s'(m) = s(A), \) it follows that

\[(5.2) \quad s'(m) = q^{m-2} \cdot s'(m - 1) \quad (m \geq 2). \]
Since \( s'(1) = 1 \), we see that (5.2) implies
\[
(5.3) \quad s'(m) = q^{(m-1)(m-2)/2} \quad (m \geq 1).
\]

Similarly if \( s(m) \) denotes the number of solutions of (5.1) in which the \( U_i \) are no longer required to be primary we find that
\[
s(m) = (q - 1)^{\lfloor m/2 \rfloor} q^{(m-1)(m-2)/2},
\]
where \( \lfloor m/2 \rfloor \) is the greatest integer \( \leq m/2 \).

In the same way we can consider special partitions of higher degree.

REFERENCES