THE DISTRIBUTION OF IRREDUCIBLE POLYNOMIALS IN SEVERAL INDETERMINATES OVER A FINITE FIELD

by STEPHEN D. COHEN

(Received 22nd February 1967)

1. Introduction

We consider non-zero polynomials $f(x_1, \ldots, x_k)$ in k variables $x_1, \ldots, x_k$ with coefficients in the finite field $GF[q]$ ($q = p^n$ for some prime p and positive integer n). We assume that the polynomials have been normalised by selecting one polynomial from each equivalence class with respect to multiplication by non-zero elements of $GF[q]$. By the degree of a polynomial $f(x_1, \ldots, x_k)$ will be understood the ordered set $(m_1, \ldots, m_k)$, where m_i is the degree of $f(x_1, \ldots, x_k)$ in x_i ($i = 1, 2, \ldots, k$). The degree $(m_1, \ldots, m_k)$ of a polynomial will be called totally positive if $m_i > 0$, $i = 1, 2, \ldots, k$.

We investigate here the number of normalised irreducible polynomials distributed among all the normalised polynomials $f(x_1, \ldots, x_k)$ of degree $(m_1, \ldots, m_k)$. Let $N(m_1, \ldots, m_k)$ denote the number of normalised polynomials of degree $(m_1, \ldots, m_k)$ in k variables $x_1, \ldots, x_k$ and $M(m_1, \ldots, m_k)$ the corresponding number of irreducibles. When $k = 1$, $M(m)$ can be evaluated explicitly and is given by

$$M(m) = \frac{1}{m} \sum_{rs = m} \mu(r) q^s, \tag{1.1}$$

where $\mu(r)$ is the Möbius function. It follows from (1.1) that

$$M(m) \sim \frac{1}{m} q^m = \frac{1}{m} N(m), \quad (m \to \infty), \tag{1.2}$$

for fixed q. More generally, Carlitz (**1**) has proved that, if $k \geqq 1$, $N_k(m)$ is the number of normalised polynomials in $x_1, \ldots, x_k$ which split into m linear factors in some extension of $GF[q]$ and in which x_k^m actually appears, and $M_k(m)$ is the corresponding number of irreducible polynomials, then $N_k(m)$ and $M_k(m)$ are given by

$$N_k(m) = q^{km}$$

and

$$M_k(m) = \frac{1}{m} \sum_{rs = m} \mu(r) q^{km}. \tag{1.3}$$

Hence

$$M_k(m) \sim \frac{1}{m} N_k(m), \quad (m \to \infty) \tag{1.4}$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

holds for all $k \geqq 1$ and fixed q. When $k \geqq 2$ and we consider *all* polynomials of degree $(m_1, \ldots, m_k)$, the situation is different and much more difficult. In this case, no explicit formula corresponding to (1.1) or (1.3) is available. Carlitz (2) has shown that, in contrast to (1.2) and (1.4), when $k \geqq 2$, in a certain sense, " almost all " polynomials are irreducible. Carlitz (3) has studied the case $k = 2$ in greater detail. Here we obtain the corresponding results for a general $k(\geqq 2)$. We shall assume from now on that $k \geqq 2$. We shall show, for example, that for fixed $m_1, \ldots, m_{k-1}$, numbered so that

$$m_{k-1} = \max_{1 \leqq i \leqq k-1} m_i,$$

$$M(m_1, \ldots, m_k) = (1-q^{-n_k})N(m_1, \ldots, m_k)+O(m_k q^{(m_1+1)\ldots(m_{k-2}+1)m_{k-1}m_k}), \quad (1.5)$$

where

$$n_k = \left\{\prod_{t=1}^{k-1} (m_t+1)\right\} -1,$$

and the constant in the O-term is independent of m_k. We shall see later that

$$N(m_1, \ldots, m_k) = O(q^{(m_1+1)\ldots(m_k+1)}),$$

where the constant implied by the O-term depends only on q. We examine results like (1.5) more closely obtaining improvements in most cases. We conclude by giving some examples.

2. Fundamental formula

The following lemma is an extension of the corresponding result for $k = 2$ in (3).

Lemma 1. *We have*

$$m_1 N(m_1, \ldots, m_k) = \sum_{r_1=0}^{m_1} \cdots \sum_{r_k=0}^{m_k} r_1 L(r_1, \ldots, r_k) N(m_1-r_1, \ldots, m_k-r_k), \quad (2.1)$$

where

$$L(r_1, \ldots, r_k) = \sum_{j \mid (r_1, \ldots, r_k)} \frac{1}{j} M\left(\frac{r_1}{j}, \ldots, \frac{r_k}{j}\right). \quad (2.2)$$

[It will be necessary to distinguish by context the degree $(r_1, \ldots, r_k)$ and the symbol $(r_1, \ldots, r_k)$ meaning the greatest common divisor of $r_1, \ldots, r_k$.]

Proof. Put

$$F(m_1, \ldots, m_k) = \Pi f(x_1, \ldots, x_k), \quad (2.3)$$

where the product extends over all normalised polynomials of degree $(m_1, \ldots, m_k)$; also put

$$P(m_1, \ldots, m_k) = \Pi p(x_1, \ldots, x_k), \quad (2.4)$$

where now the product is restricted to the normalised irreducibles of degree $(m_1, \ldots, m_k)$. If f is an arbitrary polynomial of degree $(m_1, \ldots, m_k)$ and p is an irreducible polynomial of degree $(r_1, \ldots, r_k)$, we may put

$$f = p^e g (p \nmid g),$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

where e is a non-negative integer. Let $\Phi(j_1, \ldots, j_k;\ p)$ denote the number of normalised polynomials of degree $(j_1, \ldots, j_k)$ that are not divisible by p. Then it follows from (2.3) that

$$F(m_1, \ldots, m_k) = \prod_{e,\, p} p^{e\Phi(m_1-er_1, \ldots, m_k-er_k;\ p)}, \tag{2.5}$$

where the product is over all e, r_1, ..., r_k and all irreducibles p of degree $(r_1, \ldots, r_k)$ such that $er_1 \leqq m_1$, ..., $er_k \leqq m_k$. Moreover, it is evident from the definition of $\Phi(m_1, \ldots, m_k;\ p)$ that

$$\Phi(m_1, \ldots, m_k;\ p) = N(m_1, \ldots, m_k) - N(m_1-r_1, \ldots, m_k-r_k),$$

provided $m_1 \geqq r_1$, ..., $m_k \geqq r_k$; otherwise

$$\Phi(m_1, \ldots, m_k;\ p) = N(m_1, \ldots, m_k).$$

Thus (2.5) becomes

$$F(m_1, \ldots, m_k) = \prod_{r_1=0}^{m_1} \cdots \prod_{r_k=0}^{m_k} \prod p^w, \tag{2.6}$$

where

$$\begin{aligned} w &= \sum_e e\Phi(m_1-er_1, \ldots, m_k-er_k;\ p) \\ &= \{N(m_1-r_1, \ldots, m_k-r_k) - N(m_1-2r_1, \ldots, m_k-2r_k)\} \\ &\quad + 2\{N(m_1-2r_1, \ldots, m_k-2r_k) - N(m_1-3r_1, \ldots, m_k-3r_k)\} \\ &\quad + \ldots + hN(m_1-hr_1, \ldots, m_k-hr_k), \end{aligned}$$

where h is the largest integer such that $hr_1 \leqq m_1$, ..., $hr_k \leqq m_k$. Thus

$$w = \sum_{j=1}^{h} N(m_1-jr_1, \ldots, m_k-jr_k), \tag{2.7}$$

so that (2.6) becomes

$$F(m_1, \ldots, m_k) = \prod_{r_1=0}^{m_1} \cdots \prod_{r_k=0}^{m_k} (P(r_1, \ldots, r_k))^w, \tag{2.8}$$

with w defined by (2.7) and $P(r_1, \ldots, r_k)$ by (2.4). Clearly the degree in x_1 of $F(m_1, \ldots, m_k)$ is $m_1N(m_1, \ldots, m_k)$, while the degree in x_1 of $P(r_1, \ldots, r_k)$ is $r_1M(r_1, \ldots, r_k)$. Hence (2.8) yields

$$\begin{aligned} &m_1N(m_1, \ldots, m_k) \\ &= \sum_{r_1=0}^{m_1} \cdots \sum_{r_k=0}^{m_k} r_1M(r_1, \ldots, r_k) \sum_{j=1}^{h} N(m_1-jr_1, \ldots, m_k-jr_k) \\ &= \sum_{u_1=0}^{m_1} \cdots \sum_{u_k=0}^{m_k} N(m_1-u_1, \ldots, m_k-u_k) \sum_{j \mid (u_1, \ldots, u_k)} \frac{u_1}{j} M\left(\frac{u_1}{j}, \ldots, \frac{u_k}{j}\right) \\ &= \sum_{u_1=0}^{m_1} \cdots \sum_{u_k=0}^{m_k} u_1N(m_1-u_1, \ldots, m_k-u_k)L(u_1, \ldots, u_k), \end{aligned}$$

where $L(u_1, \ldots, u_k)$ is defined by (2.2). This completes the proof of the lemma.

We note that equating the degrees in x_i $(i = 2, \ldots, k)$ in (2.8) yields only those companion formulae to (2.1) obtainable by symmetry.

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

3. Further preliminaries

Before applying Lemma 1, we require some further notation and preliminary results. For convenience, we shall assume that $(m_1, \ldots, m_k)(k \geqq 2)$ is totally positive.

Let n, i be integers with $1 \leqq i \leqq n$. In what follows, we shall denote by $\sum'_{n,i}$ a sum over all distinct selections (disregarding order) of i elements, $j_1, \ldots, j_i$, out of the set $\{1, 2, \ldots, n\}$. The remaining $n-i$ elements (in any order) will be denoted by $j_{i+1}, \ldots, j_n$.

We define Σ_t and $\sum_{\substack{t\\1}}$ to be the sum over r_{j_t} as r_{j_t} takes integral values from 0 to $m_{j_t}-1$ and from 1 to $m_{j_t}-1$, respectively. Here, as usual, empty sums are taken to be zero. We denote the multiple sums $\Sigma_1 \ldots \Sigma_i$ and $\underset{1}{\sum}_1 \ldots \underset{1}{\sum}_i$ by $\Sigma^{(i)}$ and $\underset{1}{\sum}^{(i)}$, respectively. Write

$$Q_0 = q^{(m_1+1)\ldots(m_k+1)}$$

$$Q_i = \sum_{k,i}{}' q^{m_{j_1}\ldots m_{j_i}(m_{j_{i+1}}+1)\ldots(m_{j_k}+1)}, \quad (i = 1, \ldots, k).$$

Then the function $N(m_1, \ldots, m_k)$ has the properties given in Lemma 2 below.

Lemma 2. *We have*

$$(q-1)N(m_1, \ldots, m_k) = \sum_{i=0}^{k} (-1)^i Q_i. \tag{3.1}$$

Moreover,

$$N(m_1, \ldots, m_k) = O(Q_0), \tag{3.2}$$

and

$$N(m_1, \ldots, m_k) - qN(m_1, \ldots, m_k-1) = (1-q^{-n_k})N(m_1, \ldots, m_k) + \sum_{j=1}^{k-1} O(q^{m_j m_k (m_j+1)^{-1}(n_k+1)}), \tag{3.3}$$

where

$$n_k = \left\{\prod_{t=1}^{k-1} (m_t+1)\right\} -1, \tag{3.4}$$

and the constants implied by the O-terms depend only on q.

Proof. In this proof we shall be considering only polynomials of degree at most m_i in x_i $(i = 1, \ldots, k)$. By the principal terms of a polynomial $f(x_1, \ldots, x_k)$ of degree $(m_1, \ldots, m_k)$, we shall mean those terms of $f(x_1, \ldots, x_k)$ which contain $x_j^{m_j}$ for at least one j, $1 \leqq j \leqq k$. Thus, $N(m_1, \ldots, m_k)$ is the number of normalised polynomials which contain at least one principal term involving $x_i^{m_i}$ for each i, $i = 1, \ldots, k$.

Now, for each i, with $0 \leqq i \leqq k$, the number of polynomials in which $x_1, \ldots, x_i$ (say) do not appear to the m_ith power and in which the coefficients of principal terms not involving $x_1^{m_1}, \ldots, x_i^{m_i}$ may be zero is

$$q^{m_1 \ldots m_i (m_{i+1}+1)\ldots(m_k+1)}, \quad i = 0, \ldots, k \tag{3.5}$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

(with obvious conventions for $i = 0$ or k). The sum, for fixed i, of all terms of the form (3.5) is Q_i $(i = 0, \ldots, k)$.

Hence, for any r, with $0 \leqq r \leqq i$, the number of times a polynomial in which exactly $x_1, \ldots, x_i$ (say) do not appear to the powers $m_1, \ldots, m_i$, respectively, is counted in the number Q_r is $\binom{i}{i-r} = \binom{i}{r}$ and so the number of times such a polynomial is counted in the sum

$$S = \sum_{r=0}^{k} (-1)^r Q_r$$

is

$$\sum_{r=0}^{i} (-1)^r \binom{i}{r} = \begin{cases} 1, & i = 0, \\ 0, & i = 1, \ldots, k. \end{cases}$$

Hence S is exactly the number of polynomials of degree $(m_1, \ldots, m_k)$. Since the number of equivalence classes is $(q-1)^{-1}S$, result (3.1) follows.

(3.2) is a simple consequence of (3.1).

For (3.3), consider

$$\begin{aligned}(q-1)&[q^{-n_k}N(m_1, \ldots, m_k) - qN(m_1, \ldots, m_k - 1)] \\ &= q^{-n_k}(q^{(m_1+1)\ldots(m_k+1)} - q^{m_1(m_2+1)\ldots(m_k+1)} - \ldots - q^{(m_1+1)\ldots(m_{k-1}+1)m_k} \\ &\qquad\qquad + \text{terms of smaller order}) \\ &- q(q^{(m_1+1)\ldots(m_{k-1}+1)m_k} - q^{m_1(m_2+1)\ldots(m_{k-1}+1)m_k} - \ldots - q^{(m_1+1)\ldots(m_{k-1}+1)(m_k-1)} \\ &\qquad\qquad + \text{terms of smaller order}),\end{aligned}$$

by (3.1). This, ignoring the terms of smaller order, equals

$$\begin{aligned}&[q^{(m_1+1)\ldots(m_{k-1}+1)m_k+1} - \ldots - q^{(m_1+1)\ldots(m_{k-1}+1)(m_k-1)+1}] \\ &\qquad - [q^{(m_1+1)\ldots(m_{k-1}+1)m_k+1} - \ldots - q^{(m_1+1)\ldots(m_{k-1}+1)(m_k-1)+1}].\end{aligned}$$

The terms displayed cancel out in pairs, and the remaining terms give rise to the error terms shown in (3.3) (on dividing by $q-1$). The result (3.3) follows. This completes the proof of the lemma.

Note. For large q,

$$N(m_1, \ldots, m_k) = O(q^{(m_1+1)\ldots(m_k+1)-1}).$$

In the present context q is fixed.

From Lemma 1 and (3.2), we have

$$L(m_1, \ldots, m_k) \leqq N(m_1, \ldots, m_k) = O(q^{(m_1+1)\ldots(m_k+1)}). \tag{3.6}$$

We shall use (3.6) later in the estimation of $L(m_1, \ldots, m_k)$.

Now, for fixed positive integers $m_1, \ldots, m_k$ and non-negative integers $r_1, \ldots, r_k$ write

$$T(r_1, \ldots, r_k) = (r_1+1)\ldots(r_k+1) + (m_1 - r_1 + 1)\ldots(m_k - r_k + 1)$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

so that, by (3.6),

$$L(r_1, \ldots, r_k)N(m_1-r_1, \ldots, m_k-r_k)$$

$$\leqq N(r_1, \ldots, r_k)N(m_1-r_1, \ldots, m_k-r_k) = O(q^{T(r_1, \ldots, r_k)}). \qquad (3.7)$$

The following properties of $T(r_1, \ldots, r_k)$ are immediate; viz.

$$T(r_{j_1}, \ldots, r_{j_k}) = T(r_1, \ldots, r_k), \qquad (3.8)$$

for any permutation $\{j_1, \ldots, j_k\}$ of $\{1, \ldots, k\}$, the m_i's being permuted in the same way, and

$$T(m_1-r_1, \ldots, m_k-r_k) = T(r_1, \ldots, r_k). \qquad (3.9)$$

We shall require upper bounds for terms of the form (3.7); we obtain these in Lemmas 3 and 4 below.

Lemma 3. *Let $m_1, \ldots, m_k, u$ be fixed positive integers such that $1 \leqq u \leqq k-1$, $m_t \geqq 2 (u<t \leqq k)$. Suppose also that $s_1, \ldots, s_k$ are integers satisfying*

$$\left.\begin{array}{ll} 0 \leqq s_t \leqq m_t, & (1 \leqq t \leqq u), \\ 1 \leqq s_t \leqq m_t-1, & (u < t \leqq k); \end{array}\right\} \qquad (3.10)$$

then

$$T(s_1, \ldots, s_k) \leqq T(m_1, \ldots, m_u, m_{u+1}-1, \ldots, m_k-1). \qquad (3.11)$$

Proof. To prove (3.11), we observe that if $2s_t \geqq m_t$, $t = 1, \ldots, k$, then, for each j with $1 \leqq j \leqq k$,

$$\frac{\partial T}{\partial s_j}(s_1, \ldots, s_k) = \frac{1}{s_j+1}\prod_{t=1}^{k}(s_t+1) - \frac{1}{m_j-s_j+1}\prod_{t=1}^{k}(m_t-s_t+1) \geqq 0$$

at the point $(s_1, \ldots, s_k)$. Thus T is increasing with respect to s_j for each j, $1 \leqq j \leqq k$. Hence for this case (3.11) holds.

We now show that for general $s_1, \ldots, s_k$ satisfying (3.10), there exist integers $s'_1, \ldots, s'_k$ also satisfying (3.10) with, in addition, $2s'_t \geqq m_t (t = 1, \ldots, k)$ and

$$T(s_1, \ldots, s_k) \leqq T(s'_1, \ldots, s'_k). \qquad (3.12)$$

Thus, by the first part of the proof applied to $T(s'_1, \ldots, s'_k)$ and (3.12), (3.11) is proved.

Let v be the number of the $s_t (t = 1, \ldots, k)$ such that $2s_t \geqq m_t$ and so $0 \leqq v \leqq k$. We have already discussed the case $v = k$ and the case $v = 0$ reduces to it on application of (3.9) and noting that (3.10) remains valid with s_t replaced by $m_t-s_t (t = 1, \ldots, k)$. Suppose now that $v \neq 0$, k and let $s_{j_1}, \ldots, s_{j_k}$ be a rearrangement of $s_1, \ldots, s_k$ such that $2s_{j_i} \geqq m_{j_i} (1 \leqq i \leqq v)$ and $2s_{j_i} < m_{j_i} (v+1 \leqq i \leqq k)$. Now, if s_t satisfies one of the pair of inequalities in (3.10), m_t-s_t satisfies the same inequality. Further $2(m_{j_i}-s_{j_i}) \geqq m_{j_i}$,

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

$v+1 \leqq i \leqq k$. Hence

$$T(s_{j_1}, \ldots, s_{j_v}, m_{j_{v+1}}-s_{j_{v+1}}, \ldots, m_{j_k}-s_{j_k})-T(s_{j_1}, \ldots, s_{j_k})$$
$$=\left\{\prod_{i=1}^{v}(s_{j_i}+1)-\prod_{i=1}^{v}(m_{j_i}-s_{j_i}+1)\right\}\left\{\prod_{i=v+1}^{k}(m_{j_i}-s_{j_i}+1)-\prod_{i=v+1}^{k}(s_{j_i}+1)\right\}$$
$$\geqq 0.$$

Whence (3.12) holds with

$$s'_{j_i}=\begin{cases} s_{j_i}, \ 1 \leqq i \leqq v, \\ m_{j_i}-s_{j_i}, \ v+1 \leqq i \leqq k, \end{cases}$$

after using the permutation rule (3.8). This completes the proof.

Lemma 4. *Let $m_1, \ldots, m_k, u$ be fixed positive integers with $1 \leqq u \leqq k-1$. Then*

$$T(m_1, \ldots, m_u, 0, \ldots, 0)$$
$$\leqq \max\{T(m_1, \ldots, m_u, m_{u+1}-1, \ldots, m_k-1),$$
$$T(m_1-1, \ldots, m_u-1, m_{u+1}, \ldots, m_k)\}. \qquad (3.13)$$

Proof. (i) Suppose first that $2u \geqq k$. Then

$$T(m_1, \ldots, m_u, m_{u+1}-1, \ldots, m_k-1)-T(m_1, \ldots, m_u, 0, \ldots, 0)$$
$$=(m_1+1)\ldots(m_u+1)(m_{u+1}\ldots m_k-1)-[(m_{u+1}+1)\ldots(m_k+1)-2^{k-u}]$$
$$\geqq 2^u(m_{u+1}\ldots m_k-1)-2^{k-u}(m_{u+1}\ldots m_k-1)$$
$$\geqq 0.$$

(ii) Suppose now that $2u<k$. By (3.9), (3.8)

$$T(m_1, \ldots, m_u, 0, \ldots, 0)=T(0, \ldots, 0, m_{u+1}, \ldots, m_k)$$
$$=T(m_{u+1}, \ldots, m_k, 0, \ldots, 0)$$
$$\leqq T(m_{u+1}, \ldots, m_k, m_1-1, \ldots, m_u-1),$$

by (i), since $2(k-u)>k$.

This completes the proof.

Evidently,

$$T(m_1, \ldots, m_u, m_{u+1}-1, \ldots, m_k-1)=(m_1+1)\ldots(m_u+1)m_{u+1}\ldots m_k+O(1). \qquad (3.14)$$

In fact, the constant in (3.14) is 2^{k-u}.

4. Estimation of $M(m_1, \ldots, m_k)$

It may be verified by direct substitution that we can rewrite (2.2) as

$$M(m_1, \ldots, m_k)=\sum_{j \mid (m_1, \ldots, m_k)} \frac{\mu(j)}{j} L\left(\frac{m_1}{j}, \ldots, \frac{m_k}{j}\right), \qquad (4.1)$$

where $\mu(j)$ is the Möbius function.

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

Using the results of §§ 2-3, we obtain an estimate for $L(m_1, \ldots, m_k)$ and invoke (4.1) to deduce the corresponding estimate for $M(m_1, \ldots, m_k)$. We restrict ourselves again, without loss of generality, to the case $(m_1, \ldots, m_k)$ totally positive.

We recall, from Lemma 1,

$$\begin{aligned} m_1 N(m_1, \ldots, m_k) &= \sum_{r_1=0}^{m_1} \cdots \sum_{r_k=0}^{m_k} r_1 L(r_1, \ldots, r_k) N(m_1 - r_1, \ldots, m_k + r_k) \\ &= m_1 \sum_{r_k=0}^{m_k} L(m_1, \ldots, m_{k-1}, r_k) N(0, \ldots, 0, m_k - r_k) + m_1 E, \end{aligned} \tag{4.2}$$

where, since $r_1/m_1 \leqq 1$, we have

$$\begin{aligned} E \leqq \sum_{i=1}^{k-1} \sum_{k-1,i}' \sum^{(i)} \sum_{r_k=0}^{m_k} \{ & L(r_{j_1}, \ldots, r_{j_i}, m_{j_{i+1}}, \ldots, m_{j_{k-1}}, r_k) \\ & \times N(m_{j_1} - r_{j_1}, \ldots, m_{j_i} - r_{j_i}, 0, \ldots, 0, m_k - r_k) \}. \end{aligned}$$

Using (3.7), we obtain

$$E = \sum_{i=1}^{k-1} \sum_{k-1,i}' \sum^{(i)} \sum_{r_k=0}^{m_k} O\{q^{T(r_{j_1}, \ldots, r_{j_i}, m_{j_{i+1}}, \ldots, m_{j_{k-1}}, r_k)}\}, \tag{4.3}$$

where the implied constants depend only on q. We divide the summation of (4.3) into two cases:

(i) $r_{j_t} = 0 \ (t = 1, \ldots, i)$. These terms are restated in (4.5) below. Since the summand in (2.1) contains the factor r_1 we can neglect terms in which r_1 takes the value zero in (4.3). This justifies the omission of the term

$$\sum_{r_k=0}^{m_k} O(q^{T(0, \ldots, 0, m_k)})$$

from the second multiple sum of (4.5).

(ii) $r_{j_t} \geqq 1$, for some t with $1 \leqq t \leqq i$. On application of Lemma 3, these terms give rise to a sum

$$\sum_{i=1}^{k-1} \sum_{k-1,i}' \sum_{s=1}^{i-1} \sum_{i,s}' \sum_1^{(j_s)} \sum_{r_k=0}^{m_k} O\{q^{T(m_{(1)}-1, \ldots, m_{(s)}-1, m_{(s+1)}, \ldots, m_k)}\}, \tag{4.4}$$

where the subscript (t) in $m_{(t)}$ denotes j_{j_t}. The sum (4.4) can be rewritten to give the first multiple sum in the expression

$$\begin{aligned} E = \sum_{i=1}^{k-1} \alpha_i \sum_{k-1,i}' \sum_1^{(i)} \sum_{r_k=0}^{m_k} & O\{q^{T(m_{j_1}-1, \ldots, m_{j_i}-1, m_{j_{i+1}}, \ldots, m_k)}\} \\ & + \sum_{i=1}^{k-2} \sum_{k-1,i}' \sum_{r_k=0}^{m_k} O\{q^{T(0, \ldots, 0, m_{j_{i+1}}, \ldots, m_k)}\}, \end{aligned} \tag{4.5}$$

where, for $1 \leqq i \leqq k-1$, we have

$$\alpha_i = 1 + \binom{k-1-i}{1} + \binom{k-1-i}{2} + \ldots + \binom{k-1-i}{k-1-i}$$
$$= 2^{k-1-i}.$$

Application of Lemma 4 and (3.14) to (4.5) yields

$$E = \sum_{i=1}^{k-1} \sum_{k-1,\,i}' O(m_{j_1} \ldots m_{j_i} q^{m_{j_1} \ldots m_{j_i} (m_{j_{i+1}}+1) \ldots (m_k+1)}), \tag{4.6}$$

where the constants implied by the O-terms are of the form $\beta_i B$, where B depends only on q and, for $1 \leqq i \leqq k-1$,

$$\beta_i = \begin{cases} (\alpha_i + 1) q^{2^i}, & 2i \leqq k \\ \alpha_i q^{2^i} + q^{2^{k-i}}, & 2i > k \end{cases}$$
$$\leqq (2^{k-1-i}+1) q^{2^i}.$$

For fixed k, we can neglect many of the terms in (4.6) and, in fact, obtain

$$E = \sum_{i=1}^{[k-1} O(m_i m_k q^{m_i (m_i+1)^{-1} (n_k+1)(m_k+1)}), \tag{4.7}$$

where n_k is given by (3.4) and the implied constants depend only on q and k.

Accordingly, by (4.2) and (4.7),

$$N(m_1, \ldots, m_k) = \sum_{r_k=0}^{m_k} q^{m_k - r_k} L(m_1, \ldots, m_{k-1}, r_k) + \sum_{i=1}^{k-1} O(c_i), \tag{4.8}$$

where, for $1 \leqq i \leqq k-1$,

$$c_i = m_i m_k q^{m_i (m_i+1)^{-1} (n_k+1)(m_k+1)}$$

and the constants implied by the O-terms depend only on q and k. It follows from (4.8) that, if $m_k \geqq 2$,

$$N(m_1, \ldots, m_k) - qN(m_1, \ldots, m_k - 1) = L(m_1, \ldots, m_k) + \sum_{i=1}^{k-1} O(c_i). \tag{4.9}$$

Comparing (3.3) and (4.9) we obtain

$$L(m_1, \ldots, m_k) = (1 - q^{-n_k}) N(m_1, \ldots, m_k) + \sum_{i=0}^{k-1} O(c_i). \tag{4.10}$$

Now, if $(m_1, \ldots, m_k) = 1$, i.e. if $m_1, \ldots, m_k$ are relatively prime, it follows from (4.1) that

$$M(m_1, \ldots, m_k) = L(m_1, \ldots, m_k). \tag{4.11}$$

In particular (4.11) holds when $m_j = 1$ for some j, $1 \leqq j \leqq k$. If $m_j \geqq 2$, $j = 1, \ldots, k$, we have from (4.1) and (3.6)

$$M(m_1, \ldots, m_k) = L(m_1, \ldots, m_k) + O(q^{(m_1+2) \ldots (m_k+2)/2^k})$$
$$= L(m_1, \ldots, m_k) + O(q^{m_1 \ldots m_k}). \tag{4.12}$$

Thus, combining (4.11) and (4.12), (4.12) holds for all totally positive $(m_1, \ldots, m_k)$. Here again the implied constant depends only on q.

From (4.10) and (4.12), we obtain an expression for $M(m_1, \ldots, m_k)$ which is the main result of the following theorem.

Theorem 1. *Let $m_1, \ldots, m_k$ be positive integers with $k \geqq 2$. Then the number $M(m_1, \ldots, m_k)$ of normalised irreducible polynomials of degree $(m_1, \ldots, m_k)$ in k indeterminates with coefficients in $GF[q]$ satisfies*

$$M(m_1, \ldots, m_k) = (1-q^{-n_k})N(m_1, \ldots, m_k) + \sum_{i=1}^{k-1} O(m_i m_k q^{m_i(m_i+1)^{-1}(n_k+1)(m_k+1)}), \qquad (4.13)$$

where $N(m_1, \ldots, m_k)$ is the total number of normalised polynomials of degree $(m_1, \ldots, m_k)$, n_k is given by (3.4) *and the constants implied by the O-terms depend only on the field* (i.e. *on q*) *and on k.*

In particular, for fixed $m_1, \ldots, m_{k-1}$, numbered so that

$$m_{k-1} = \max_{1 \leqq i \leqq k-1} m_i,$$

$$M(m_1, \ldots, m_k) = (1-q^{-n_k})N(m_1, \ldots, m_k) + O(m_k q^{(m_1+1)\ldots(m_{k-2}+1)m_{k-1}m_k}), \qquad (4.14)$$

where the implied constant is independent of m_k; and

$$M(m_1, \ldots, m_k) \sim (1-q^{-n_k})N(m_1, \ldots, m_k) \text{ as } m_k \to \infty. \qquad (4.15)$$

Further, for $k \geqq 3$ and fixed $m_1, \ldots, m_{k-2}$,

$$M(m_1, \ldots, m_k) \sim N(m_1, \ldots, m_k) \text{ as } m_{k-1}, m_k \to \infty. \qquad (4.16)$$

Proof. We have already proved (4.13). Statements (4.14) and (4.15) are immediate from (4.13). Also (4.16) follows from (4.15) on observing that, for fixed $m_1, \ldots, m_{k-2}$,

$$q^{-n_k}N(m_1, \ldots, m_k) = o(N(m_1, \ldots, m_k)) \text{ as } m_{k-1}, m_k \to \infty.$$

This completes the proof.

We note that, by (4.16), we can say that, if $2 \leqq j \leqq k$,

$$M(m_1, \ldots, m_k) \sim N(m_1, \ldots, m_k) \quad (k \geqq 2)$$

holds as any j of $m_1, \ldots, m_k \to \infty$.

We investigate (4.14) and (4.16) in more detail in § 5 below.

5. Improvement of (4.14) and (4.16)

We consider first the estimation of $M(m_1, \ldots, m_k)$ in which $m_1, \ldots, m_{k-1}$ are fixed. In this case we can improve (4.14) except when $k = 2$ and $m_1 = 2$ and when $k = 3$ and $m_1 = m_2 = 1$.

We can calculate $M(2, n)$ and $M(1, 1, n)$, where $n \geqq 1$, directly using Lemma 1 and (4.1) (see § 6). When expressed in the form of (4.14), we obtain

$$M(2, n) = (1-q^{-2})N(2, n) - \tfrac{1}{2}q^2(1-q^{-2})^2 nq^{2n} + O(q^{2n}),$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

and

$$M(1,\,1,\,n)=(1-q^{-3})N(1,\,1,\,n)-q^2(1-q^{-2})^2nq^{2n}+O(q^{2n}),$$

both expressions being valid for large n. We see that in these cases (4.14) is " best possible ".

Define the positive integer R by

$$\left.\begin{aligned} R&=1, \text{ if } k=2,\\ R&=(m_1+1)\ldots(m_{k-2}+1), \text{ if } k\geqq 3. \end{aligned}\right\} \tag{5.1}$$

Then apart from the cases already considered we may replace (4.14) by the improvement contained in the following theorem.

Theorem 2. *Let $m_1,\,\ldots,\,m_{k-1}(k\geqq 2)$ be fixed positive integers numbered so that $m_1\leqq m_2\leqq\ldots\leqq m_{k-1}$. Then, in the notation of Theorem 1, $M(m_1,\,\ldots,\,m_k)$ satisfies, with the exceptions of $M(2,\,m_2)$ and $M(1,\,1,\,m_3)$,*

$$M(m_1,\,\ldots,\,m_k)=(1-q^{-n_k})N(m_1,\,\ldots,\,m_k)+O(q^{Rm_{k-1}m_k}), \tag{5.2}$$

for large m_k, where R is given by (5.1) and the implied constant is independent of m_k. Further, (5.2) is the " best possible " estimate for $M(m_1,\,\ldots,\,m_k)$, i.e., there exists a positive number K, independent of m_k, such that, for fixed $m_1,\,\ldots,\,m_{k-1}$,

$$\left|\,M(m_1,\,\ldots,\,m_k)-(1-q^{-n_k})N(m_1,\,\ldots,\,m_k\,\right|>Kq^{Rm_{k-1}m_k} \tag{5.3}$$

holds.

Proof. In this proof let Δ denote the difference

$$N(m_1,\,\ldots,\,m_k)-qN(m_1,\,\ldots,\,m_k-1).$$

We require the following consequences of (3.1), valid for large m_k. We have

$$\begin{aligned} N(m_1,\,\ldots,\,m_{k-2},\,m_{k-1}-1,\,m_k)=(q-1)^{-1}&(q^{Rm_{k-1}}-1)q^{Rm_{k-1}m_k}\\ &+O(q^{R(m_{k-1}-1)m_k}), \end{aligned} \tag{5.4}$$

and

$$\begin{aligned} \Delta=(1-q^{-n_k})&N(m_1,\,\ldots,\,m_k)\\ &+(1-q^{-1})^{-1}(1-q^{-R})(1-q^{-Rm_{k-1}})q^{Rm_{k-1}m_k}+o(q^{Rm_{k-1}m_k}). \end{aligned} \tag{5.5}$$

We verify (5.4) and (5.5) as follows. Firstly, by (3.1), we have

$$\begin{aligned} (q-1)N(m_1,\,\ldots,\,m_k)&=q^{R(m_{k-1}+1)(m_k+1)}-q^{R(m_{k-1}+1)m_k}+O(q^{Rm_{k-1}m_k})\\ &=(q^{R(m_{k-1}+1)}-1)q^{R(m_{k-1}+1)m_k}+O(q^{Rm_{k-1}m_k}). \end{aligned}$$

This gives (5.4) (on replacing m_{k-1} by $m_{k-1}-1$). To prove (5.5), consider the expression E_1, where

$$E_1=\Delta-(1-q^{-n_k})N(m_1,\,\ldots,\,m_k).$$

Then

$$E_1=q^{-n_k}N(m_1,\,\ldots,\,m_k)-qN(m_1,\,\ldots,\,m_k-1).$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

Thus, by (3.1),

$$\begin{aligned}(q-1)E_1 = q^{-R(m_{k-1}+1)+1}[q^{R(m_{k-1}+1)(m_k+1)} - q^{R(m_{k-1}+1)m_k} - q^{Rm_{k-1}(m_k+1)} \\ + q^{Rm_{k-1}m_k} + o(q^{Rm_{k-1}m_k})] \\ - q[q^{R(m_{k-1}+1)m_k} - q^{R(m_{k-1}+1)(m_k-1)} - q^{Rm_{k-1}m_k} + q^{Rm_{k-1}(m_k-1)} + o(q^{Rm_{k-1}m_k})].\end{aligned}$$

The first two terms in the first large bracket cancel with the corresponding terms in the second large bracket as in the proof of Lemma 2. Hence, ignoring the o-terms, we have

$$\begin{aligned}(q-1)E_1 &= q^{Rm_{k-1}m_k+1}[-q^{-R} + q^{-R(m_{k-1}+1)} + 1 - q^{-Rm_{k-1}}] \\ &= q^{Rm_{k-1}m_k+1}(1-q^{-R})(1-q^{-Rm_{k-1}}),\end{aligned}$$

which yields (5.5) on division by $q-1$.

Now, from (4.2), Δ is also given by

$$\begin{aligned}\Delta = L(m_1, \ldots, m_k) \\ + \sum_{i=1}^{k-1} \sum_{k-1,i}' \sum^{(i)} \sum_{r_k=0}^{m_k} \left[\left\{\frac{r_1}{m_1} L(r_{j_1}, \ldots, r_{j_i}, m_{j_{i+1}}, \ldots, m_{j_{k-1}}, r_k)\right\}\right] \\ \times \{N(m_{j_1}-r_{j_1}, \ldots, m_{j_i}-r_{j_i}, 0, \ldots, 0, m_k-r_k) \\ -qN(m_{j_1}-r_{j_1}, \ldots, m_{j_i}-r_{j_i}, 0, \ldots, 0, m_k-r_k-1)\} \\ + \sum_{i=1}^{k-1} \sum_{k-1,i}' \sum^{(i)} \left[\left\{\frac{r_1}{m_1} L(r_{j_1}, \ldots, r_{j_i}, m_{j_{i+1}}, \ldots, m_{j_{k-1}}, m_k)\right\}\right. \\ \left.\times \{N(m_{j_1}-r_{j_1}, \ldots, m_{j_i}-r_{j_i}, 0, \ldots, 0)\}\right]. \qquad (5.6)\end{aligned}$$

Let α be the number of m_t, $1 \leqq t \leqq k-1$, such that $m_t = m_{k-1}$. Also define the integer t_k by

$$t_k = Rm_{k-1} - 1.$$

Then a fairly long, complicated argument, which we shall omit, shows that, except when $k = 2$ and $m_1 = 2$ and when $k = 3$ and $m_1 = m_2 = 1$, from (5.6), it follows that

$$\begin{aligned}\Delta = L(m_1, \ldots, m_k) \\ +\beta(1-q^{-1}) \sum_{r_k=0}^{m_k-1} L(m_1, \ldots, m_{k-2}, m_{k-1}-1, r_k)N(0, \ldots, 0, 1, m_k-r_k) \\ +(\alpha-\beta)(1-q^{-t_k}) \sum_{r_k=0}^{m_k-1} L(0, \ldots, 0, 1, m_k-r_k)N(m_1, \ldots, m_{k-2}, m_{k-1}-1, r_k) \\ +\beta L(m_1, \ldots, m_{k-1}-1, m_k)N(0, \ldots, 0, 1, 0) \\ +(\alpha-\beta)(1-q^{-t_k})L(0, \ldots, 0, 1, 0)N(m_1, \ldots, m_{k-1}-1, m_k)+o(q^{Rm_{k-1}m_k}), \quad (5.7)\end{aligned}$$

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

where

$$\beta = \begin{cases} \alpha - \dfrac{1}{m_1}, \text{ if } \alpha = k-1 \\ \alpha, \text{ otherwise.} \end{cases}$$

By (4.10), (2.14), (5.5) and (5.7) we have, with the same exceptions,

$$\begin{aligned} M(m_1, \ldots, m_k) &= (1-q^{-n_k})N(m_1, \ldots, m_k) \\ &-\alpha(1-q^{-1})(1-q^{-t_k}) \sum_{r_k=0}^{m_k-1} N(m_1, \ldots, m_{k-2}, m_{k-1}-1, r_k)N(0, \ldots, 0, 1, m_k-r_k) \\ &-\alpha(1-q^{-t_k})N(m_1, \ldots, m_{k-2}, m_{k-1}-1, m_k)N(0, \ldots, 0, 1, 0) \\ &+(1-q^{-1})^{-1}(1-q^{-R})(1-q^{-Rm_{k-1}})q^{Rm_{k-1}m_k}+o(q^{Rm_{k-1}m_k}). \end{aligned} \tag{5.8}$$

For the proof of (5.2), we use (5.8) in the weaker form

$$\begin{aligned} M(m_1, \ldots, m_k)-(1-q^{-n_k})N(m_1, \ldots, m_k) &= \sum_{r_k=0}^{m_k-1} O(q^{T(m_1, \ldots, m_{k-2}, m_{k-1}-1, r_k)})+O(q^{Rm_{k-1}m_k}) \\ &= O(q^{2m_k}) \sum_{r_k=0}^{m_k-1} q^{r_k(Rm_{k-1}-2)}+O(q^{Rm_{k-1}m_k}), \end{aligned} \tag{5.9}$$

where the implied constants are independent of m_k. Now $Rm_{k-1}-2 = 0$ if and only if either $R = 1$, $k = 2$ and $m_{k-1} = 2$ or $R = 2$, $k = 3$ and $m_1 = m_2 = 1$. These are the special cases already considered and excluded from this discussion. Otherwise, R.H.S. of (5.9) is

$$\begin{aligned} &O(q^{2m_k+(m_k-1)(Rm_{k-1}-2)})+O(q^{Rm_{k-1}m_k}) \\ &= O(q^{Rm_{k-1}m_k}), \end{aligned}$$

where the implied constant is independent of m_k. This proves (5.2).

To prove (5.3), we again consider (5.8). By (5.4), we have

$$N(0, \ldots, 0, 1, 0)N(m_1, \ldots, m_{k-2}, m_{k-1}-1, m_k) = (1-q^{-1})^{-1}(q^{t_k+1}-1)q^{Rm_{k-1}m_k} +o(q^{Rm_{k-1}m_k}). \tag{5.10}$$

Thus, if Δ_1 is given by

$$\Delta_1 = M(m_1, \ldots, m_k)-(1-q^{-n_k})N(m_1, \ldots, m_k),$$

it follows from (5.8) and (5.10) that

$$\begin{aligned} \Delta_1 \leqq [(1-q^{-1})^{-1}(1-q^{-R})(1-q^{-(t_k+1)}) \\ -\alpha(1-q^{-1})^{-1}(1-q^{-t_k})(q^{t_k+1}-1)]q^{Rm_{k-1}m_k}+o(q^{Rm_{k-1}m_k}) \\ = -Kq^{Rm_{k-1}m_k}+o(q^{Rm_{k-1}m_k}), \text{ say.} \end{aligned}$$

Now, $-K$ is negative except when $t_k = 0$, i.e., when $k = 2$ and $m_1 = 1$.

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

Hence, except in the case $M(1, m_2)$, we have, for large m_k,

$$|\Delta_1| \geqq Kq^{Rm_{k-1}m_k},$$

where K is positive and independent of m_k. Thus (5.3) is proved except, possibly, for $M(1, m_2)$. However, in this case, (5.3) can be verified directly. In fact,

$$M(1, \mathrm{n}) = (1-q^{-1})N(1, n)+(1-q^{-1})q^n.$$

This completes the proof of Theorem 2.

From the results of § 5, it also follows that

$$M(m_1, ..., m_k)<(1-q^{-n_k})N(m_1, ..., m_k), \tag{5.11}$$

for large m_k, except when $k = 2$ and $m_1 = 1$.

Suppose now that $k \geqq 3$ and that $m_1, ..., m_{k-2}$ are fixed, positive integers. In this case, Theorem 1 yields, for large m_{k-1} and m_k,

$$M(m_1, ..., m_k) = N(m_1, ..., m_k)-[(1-q^{-1})^{-1}+o(1)]q^{R(m_{k-1}+1)m_k} +O(m_{k-1}m_kq^{Rm_{k-1}(m_k+1)}), \tag{5.12}$$

since, by (3.1),

$$q^{-n_k}N(m_1, ..., m_k) = (1-q^{-1})^{-1}q^{R(m_{k-1}+1)m_k}+o(q^{R(m_{k-1}+1)m_k}). \tag{5.13}$$

Considerations of symmetry suggest that (5.12) can be improved to give the result of our final theorem.

Theorem 3. *Let* $m_1, ..., m_{k-2}$, *where* $k \geqq 3$, *be fixed, positive integers. Then, in the notation of Theorem* 1,

$$M(m_1, ..., m_k) = N(m_1, ..., m_k)-[(1-q^{-1})^{-1}+o(1)] (q^{R(m_{k-1}+1)m_k}+q^{Rm_{k-1}(m_k+1)})$$

holds for large m_{k-1} *and* m_k, *where R is determined by* (5.1). *In particular* (4.16) *holds.*

Proof. The result follows on letting m_{k-1} become large in (5.8) and using (5.13) and Lemma 2. By the choice of m_{k-1} in Theorem 2 as $\max m_i$, $1 \leqq i \leqq k-1$, we can see that (5.8) is valid for large m_{k-1} and m_k (i.e., provided $m_{k-1}>m_i$, $1 \leqq i \leqq k-2$). Also, we can take $\alpha = 1$ in (5.8). In the right hand side of (5.8), apart from the first term, the only term which is not

$$o(q^{Rm_{k-1}(m_k+1)})$$

is, by Lemma 2,

$$(1-q^{-t_k})N(m_1, ..., m_{k-2}, m_{k-1}-1, m_k)N(0, ..., 0, 1, 0),$$

which equals

$$(1-q^{-1})^{-1}q^{Rm_{k-1}(m_k+1)}+o(q^{Rm_{k-1}(m_k+1)}),$$

as m_{k-1} and $m_k \to \infty$. The proof is complete.

Note. Theorem 3 has been given for $k \geqq 3$ to make its statement easier.

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

In fact, the same proof for $k = 2$ shows that

$$M(m, n) = N(m, n) - [(1-q^{-1})^{-1} + o(1)](q^m + q^n)q^{mn}$$

holds as m and n tend to infinity.

6. Examples

We now list explicit values of $M(m_1, \ldots, m_k)$ for the simplest cases in which $k = 2$ or 3. They are obtained by calculating $L(m_1, \ldots, m_k)$ from (5.6), using previously calculated values of the L-function and (3.1), and then applying (4.1).

We obtain, in turn, for $n \geqq 1$,

$$M(1, n) = (q^2-1)q^{2n-1}; \tag{6.1a}$$

$$M(2, n) = (q^2-1)\{(q^2+q+1)q^{3n-2} - \tfrac{1}{2}((q^2-1)n + (q+1)^2)q^{2n-2} - \tfrac{1}{2}\delta q^{n-1}\}, \tag{6.1b}$$

where δ is 1 or 0 according as n is even or odd,

$$\begin{aligned} M(3, n) = {} & (q^2-1)\{(q^2+1)(q^2+q+1)q^{4n-3} - (q+1)^2(q^2+q+1)q^{3n-3} \\ & + \tfrac{1}{6}[(q^2-1)^2n^2 + 3(q-1)(q+1)^3 n + 2(q^2+q+1)(q^2+5q+1)]q^{2n-3} - \tfrac{1}{3}\varepsilon q^{\frac{2n}{3}-1}\}, \end{aligned} \tag{6.1c}$$

where $\varepsilon = 1$ or 0 according as 3 does or does not divide n;

$$M(1, 1, n) = (q^2-1)\{(q^2+1)(q^2+q+1)q^{4n-3} - [(q^2-1)n + (q+1)^2]q^{2n-2}\}; \tag{6.1d}$$

and

$$\begin{aligned} M(1, 2, n) = {} & (q^2-1)\{(q^4+q^2+1)(q^4+q^3+q^2+q+1)q^{6n-5} \\ & -(q^2+1)(q^2+q+1)^2q^{4n-4} - (q+1)^2(q^2+q+1)q^{3n-3} \\ & + [\tfrac{1}{2}(q^2-1)n^2 + \tfrac{3}{2}(q^2-1)(2q^2+2q-1)n + (5q^3+8q^2+5q-1)]q^{2n-3}\} \end{aligned} \tag{6.1e}$$

Thus, we have, for large n,

$$M(1, n) = (1-q^{-1})N(1, n) + (q-1)q^{n-1}, \tag{6.2a}$$

$$M(2, n) = (1-q^{-2})N(2, n) - \tfrac{1}{2}(q^2-1)^2nq^{2n-2} + O(q^{2n}), \tag{6.2b}$$

$$M(3, n) = (1-q^{-3})N(3, n) - (q^2+2q+2)(q^3-1)q^{3n-2} + O(n^2q^{2n}), \tag{6.2c}$$

$$M(1, 1, n) = (1-q^{-3})N(1, 1, n) - (q^2-1)^2nq^{2n-2} + O(q^{2n}), \tag{6.2d}$$

and

$$M(1, 2, n) = (1-q^{-5})N(1, 2, n) - (q^4-1)(q^3+2q^2+q+1)q^{4n-4} + O(q^{3n}). \tag{6.2e}$$

The above expressions illustrate Theorem 2 (and its exceptions) and also (5.11).

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press

The derivation of the above results is increasingly complicated. Each further computation, using this method, would require considerable calculation.

Finally, to illustrate Theorem 3, we estimate $M(1, n, 2n)$ for large n. For integers i, r, s with $s \geqq 1$, let $N'(i, r, s)$ denote the difference

$$N(i, r, s)-qN(i, r, s-1).$$

Then from (4.1) and (5.6) we have

$$M(1, n, 2n) = L(1, n, 2n) = N'(1, n, 2n)-\sum_{r=0}^{n-1} L(1, r, 2n)N(0, n-r, 0)$$

$$-\sum_{r=0}^{n-1}\sum_{s=0}^{2n-1} L(1, r, s)N'(0, n-r, 2n-s). \qquad (6.3)$$

Now, using an estimate for $N(1, n, 2n-1)$, we have, for large n,

$$N'(1, n, 2n) = N(1, n, 2n)-q(q-1)^{-1}(q^{4n(n+1)}-q^{2(n+1)(2n-1)}+O(q^{4n^2})).$$

With the convention that $N'(0, n-r, 0)$ is taken to mean $N(0, n-r, 0)$, it follows from (3.7) that, if $0 \leqq r \leqq n-1$ and $0 \leqq s \leqq 2n$,

$$L(1, r, s)N'(0, n-r, 2n-s) \leqq L(1, r, s)N(0, n-r, 2n-s) = O(q^{T(1, r, s)}).$$

We show that if $0 \leqq r \leqq n-1$ and $0 \leqq s \leqq 2n$ then

$$T(1, r, s) \leqq 4n^2 +O(1) \qquad (6.4)$$

for large n, except when $r = n-1$ and $s = 2n$. If

$$1 \leqq r \leqq n-1 \text{ and } 1 \leqq s \leqq 2n-1,$$

(6.4) follows from Lemma 3. Also, from the proof of Lemma 3, it is evident that, if $2 \leqq r \leqq n-2$ and $0 \leqq s \leqq 2n$, then

$$T(1, r, s) \leqq T(1, n-2, 2n) = 4n^2-2n+1$$

so that (6.4) holds in this case too. Again, if $0 \leqq r \leqq 1$ and $0 \leqq s \leqq 2n$, we have

$$\begin{aligned} T(1, r, s) &= 2(r+1)(s+1)+(n-r+1)(2n-s+1) \\ &\leqq 2(r+1)+(n-r+1)(2n+1), \quad \text{if } n \geqq 4 \\ &\leqq (n+1)(2n+1)+2, \end{aligned}$$

since the function is decreasing with respect to s for $n \geqq 4$. To complete the proof of (6.4), we observe that

$$T(1, n-1, 0) = 2n+2(2n+1) \leqq 4n^2,$$

for large n. Finally, from (4.10) and (3.1), we see that, for large n,

$$\begin{aligned} L(1, n-1, 2n)N(0, 1, 0) &= q(1-q^{-(2n-1)})(q-1)^{-1}(q^{2n(2n+1)}+O(q^{4n^2})) \\ &= q(q-1)^{-1}q^{2n(2n+1)}+O(q^{4n^2}). \end{aligned}$$

Hence, (6.3) yields, for large n,

$$M(1,\, n,\, 2n) = N(1,\, n,\, 2n) - (1-q^{-1})^{-1}q^{4n(n+1)} - [(q+1)+o(1)]q^{2n(2n+1)-1},$$

in accordance with Theorem 3.

I wish to thank Dr. John Hunter for the invaluable assistance he has given me at all stages in the preparation of this paper.

REFERENCES

(1) L. Carlitz, On factorable polynomials in several indeterminates, *Duke Math. J.*, **2** (1936), 660-670.

(2) L. Carlitz, The distribution of irreducible polynomials in several indeterminates, *Illinois J. Math.*, **7** (1963), 371-375.

(3) L. Carlitz, The distribution of irreducible polynomials in several indeterminates II, *Canadian J. Math.*, **17** (1965), 261-266.

The University
Glasgow, W.2

https://doi.org/10.1017/S001309150001213X Published online by Cambridge University Press