THE DISTRIBUTION OF IRREDUCIBLE POLYNOMIALS IN SEVERAL INDETERMINATES II

L. CARLITZ

1. It is well known that the number of normalized irreducible polynomials of degree m in a single indeterminate, with coefficients in GF(q), is given by

$$\psi_1(m) = \frac{1}{m}\sum_{rs=m}\mu(r)q^s, \tag{1.1}$$

where $\mu(r)$ is the Möbius function. It follows from (1) that

$$\psi_1(m) \sim \frac{1}{m}q^m \qquad (m \to \infty) \tag{12}$$

for fixed q. When the number of irreducibles exceeds 1 the situation is different. In the first place no explicit formula for the number of irreducible polynomials is available. Secondly "almost all" polynomials are irreducible. If $f_k(m)$ denotes the total number of normalized polynomials in k indeterminates and $\psi_k(m)$ the number of normalized irreducibles, then the writer has proved **(1)** that

$$\psi_k(m) \sim f_k(m) \qquad (k > 1, m \to \infty). \tag{1.3}$$

More precisely we have

$$\psi_k(m) = (q-1)^{-1}\exp_q\binom{m+k}{k} + O\left\{\exp_q\binom{m+k-1}{k}\right\}, \tag{1.4}$$

where

$$\exp_q a = q^a \tag{1.5}$$

and $\binom{m}{k}$ is a binomial coefficient.

It may be of interest to consider the following more refined classification of irreducible polynomials. For simplicity we confine ourselves to the case of two indeterminates. We assume that the polynomials in x, y have been normalized by selecting one polynomial from each equivalence class with respect to multiplication by non-zero numbers of GF(q). By the degree of a polynomial $A(x, y)$ will be understood the pair (m, n), where m is the degree in x and n the degree in y.

Now let $f(m, n)$ denote the number of normalized polynomials in x, y and let $\psi(m, n)$ denote the number of normalized irreducible polynomials in x, y. Then we show that, for fixed m,

Received November 19, 1963. Supported in part by National Science Foundation grant GP 1593.

$$\lim_{n=\infty} \frac{\psi(m,n)}{f(m,n)} = 1 - \frac{1}{q^m} \qquad (n \to \infty); \tag{1.6}$$

more precisely, we have

$$\psi(m,n) = (1 - q^{-m})f(m,n) + O(mq^{mn}), \tag{1.7}$$

where the constant in the O-term depends on q and m.

2. We first prove the following formula:

$$mf(m,n) = \sum_{r=0}^{m} \sum_{s=0}^{n} rg(r,s)f(m-r, n-s), \tag{2.1}$$

where

$$g(r,s) = \sum_{j|(r,s)} \frac{1}{j} \psi\left(\frac{r}{j}, \frac{s}{j}\right). \tag{2.2}$$

Put

$$F(m,n) = \prod A(x,y), \tag{2.3}$$

where the product extends over all normalized polynomials of degree (m,n); also put

$$\Theta(m,n) = \prod P(x,y), \tag{2.4}$$

where now the product is restricted to the normalized irreducible polynomials of degree (m,n). If A is an arbitrary polynomial of degree (m,n) and P an irreducible of degree (r,s) we may put

$$A = P^e B \qquad (P \nmid B).$$

Let $\Phi(j,k;P)$ denote the number of normalized polynomials of degree (j,k) that are not divisible by P. Then it follows from (2.3) that

$$F(m,n) = \prod_{e,P} P^{e\Phi(m-er,n-es;P)}, \tag{2.5}$$

where the product is over all e, r, s and all irreducibles P of degree (r,s) such that $er \leqslant m$, $es \leqslant n$. Moreover, it is evident from the definition of $\Phi(m,n;P)$ that

$$\Phi(m,n;P) = f(m,n) - f(m-r, n-s)$$

provided $m \geqslant r$, $n \geqslant s$; otherwise

$$\Phi(m,n;P) = f(m,n).$$

Thus (2.5) becomes

$$F(m,n) = \prod_{r=0}^{m} \prod_{s=0}^{n} \prod_{P} P^w, \tag{2.6}$$

where

$$w = \sum_{e} e\phi(m - er, n - es; P)$$

$$= \{f(m, n) - f(m - r, n - s)\} + 2\{f(m - r, n - s) - f(m - 2r, n - 2s)\} + \ldots + kf(m - kr, n - ks),$$

where k is the largest integer such that $kr \leqslant m$, $ks \leqslant n$. Thus

$$w = \sum_{j=1}^{k} f(m - jr, n - js), \tag{2.7}$$

so that (2.6) becomes

$$F(m, n) = \prod_{r=0}^{m} \prod_{s=0}^{n} (\Theta(r, s))^{w}, \tag{2.8}$$

with w defined by (2.7) and $\Theta(r, s)$ by (2.4).

Clearly the degree in x of $F(m, n)$ is equal to $mf(m, n)$ while the degree in x of $\Theta(r, s)$ is equal to $r\psi(r, s)$. Hence (2.8) yields

$$\begin{aligned} mf(m, n) &= \sum_{r=0}^{m} \sum_{s=0}^{n} r\psi(r, s) \sum_{j=1}^{k} f(m - jr, n - js) \\ &= \sum_{u=0}^{m} \sum_{v=0}^{n} f(m - u, n - v) \sum_{j \mid (u, v)} \frac{u}{j} \psi\left(\frac{u}{j}, \frac{v}{j}\right) \\ &= \sum_{u=0}^{m} \sum_{v=0}^{n} uf(m - u, n - v)\, g(u, v), \end{aligned}$$

where $g(r, s)$ is defined by (2.2). This completes the proof of (2.1).

Since

$$f(m, n) = f(n, m), \qquad \psi(m, n) = \psi(n, m), \qquad g(m, n) = g(n, m),$$

the companion formula

$$nf(m, n) = \sum_{r=0}^{m} \sum_{s=0}^{n} sg(r, s) f(m - r, n - s)$$

contains nothing new.

The following heuristic proof of (2.1) may be of interest. Put

$$Z(u, v) = \sum_{m, n=0} f(m, n) u^{m} v^{n}. \tag{2.9}$$

Then we have

$$Z(u, v) = \prod_{r+s>0} (1 - u^{r} v^{s})^{-\psi(r, s)},$$

so that

$$\log Z(u,v) = \sum_{r+s>0} \psi(r,s) \sum_{j=1}^{\infty} \frac{u^{jr}v^{js}}{j}$$

$$= \sum_{m+n>0} u^m v^n \sum_{j|(m,n)} \frac{1}{j} \psi\left(\frac{m}{j}, \frac{n}{j}\right)$$

$$= \sum_{m+n>0} u^m v^n g(m,n).$$

Differentiating with respect to u, we get

$$\sum_{m,n} mf(m,n)u^m v^n = \sum_{m,n} f(m,n)u^m v^n \sum_{r,s} ru^r v^s g(r,s).$$

Equating coefficients we get (2.1).

Unfortunately the series in (2.9) converges only for $x = y = 0$.

3. It is clear from the definition that

$$(q-1)f(m,n) = q^{(m+1)(n+1)} - q^{m(n+1)} - q^{(m+1)n} + q^{mn}. \tag{3.1}$$

Thus (2.1) can be used to compute $g(m,n)$.

We have

$$f(0,n) = g(0,n) = q^n. \tag{3.2}$$

Assume that $g(r,n)$ has been computed for $r < m$ and put

$$U(m,n) = mf(m,n) - \sum_{r=1}^{m-1} r \sum_{s=0}^{n} g(r,s)f(m-r, n-s).$$

Then (2.1) becomes

$$m \sum_{s=0}^{n} q^{n-s} g(m,s) = U(m,n)$$

and therefore

$$mg(m,n) = U(m,n) - qU(m,n-1). \tag{3.3}$$

For example, when $m = 1$, we get

$$g(1,n) = f(1,n) - qf(1,n-1).$$

Since

$$f(1,n) = q^{2n}(q+1) - q^n, \tag{3.4}$$

this reduces to

$$g(1,n) = q^{2n-1}(q^2-1) \qquad (n \geqslant 1). \tag{3.5}$$

It follows from (2.2) that

$$\psi(m,n) = \sum_{j|(m,n)} \frac{\mu(j)}{j} g\left(\frac{m}{j}, \frac{n}{j}\right) \tag{3.6}$$

and in particular $\psi(1, s) = g(1, s)$ so that

$$\psi(1, n) = q^{2n-1}(q^2 - 1) \qquad (n \geqslant 1). \tag{3.7}$$

Comparison of (3.7) with (3.4) gives

$$\lim_{n=1} \frac{\psi(1, n)}{f(1, n)} = 1 - \frac{1}{q}. \tag{3.8}$$

For $m = 2$ the results are considerably more complicated. For example

$$2g(2, 2) = 2q^8 + 2q^7 - 3q^6 - 4q^5 + q^4 + 2q^3 - q^2. \tag{3.9}$$

4. It is evident from (3.4) and (3.5) that

$$\sum_{s=0}^{n} g(1, s)f(1, n - s) = \sum_{s=0}^{n} O(q^{2s} \cdot q^{2n-2s}) = O(nq^{2n}).$$

Thus, for $m = 2$, (2.1) becomes

$$f(2, n) = \sum_{s=0}^{n} q^{n-s} \cdot g(2, s) + O(nq^{2n}).$$

It follows that

$$f(2, n) - qf(2, n - 1) = g(2, n) + O(nq^{2n}).$$

Also it is evident from (3.1) that

$$f(2, n) - gf(2, n - 1) = \left(1 - \frac{1}{q^2}\right) f(2, n) + O(q^{2n}).$$

Therefore

$$g(2, n) = \left(1 - \frac{1}{q^2}\right) f(2, n) + O(nq^{2n}). \tag{4.1}$$

Now let $m \geqslant 3$. It follows at once from (2.1) and (3.1) that

$$g(m, n) \leqslant f(m, n) \leqslant q^{(m+1)(n+1)}.$$

Then for $1 \leqslant r \leqslant m - 1$,

$$\begin{aligned} \sum_{s=0}^{n} g(r, s)f(m - r, n - s) &= \sum_{s=0}^{n} O(q^{(r+1)(s+1)} \cdot q^{(m-r+1)(n-s+1)}) \\ &= \sum_{s=0}^{n} O(q^{m(n+1)}) = O(nq^{mn}). \end{aligned} \tag{4.2}$$

Thus (2.1) reduces to

$$f(m, n) = \sum_{s=0}^{n} q^{n-s} \cdot g(m, s) + O(nq^{mn}). \tag{4.3}$$

Actually the constant in the O-term in (4.2) is independent of m and therefore (4.3) can be stated in the more precise form

$$f(m, n) = \sum_{s=0}^{n} q^{n-s} \cdot g(m, s) + O(mnq^{mn}), \tag{4.4}$$

where now the implied constant depends only on q. It follows from (4.4) that

$$g(m, n) = f(m, n) - gf(m, n - 1) + O(mnq^{mn}).$$

Since by (3.1)

$$f(m, n) - qf(m, n - 1) = (1 - q^{-m})f(m, n) + O(q^{m(n+1)}),$$

we get

$$g(m, n) = (1 - q^{-m})f(m, n) + O(mnq^{mn}) + O(q^{m(n+1)}). \tag{4.5}$$

If m and n are relatively prime, it follows from (3.6) that

$$\psi(m, n) = g(m, n) \qquad ((m, n) = 1). \tag{4.6}$$

In the general case we evidently have

$$\psi(m, n) = g(m, n) + O(q^{(m+2)(n+2)/4}) = g(m, n) + O(q^{mn}). \tag{4.7}$$

We may now state the following

THEOREM. *The number of normalized irreducibles of degree (m, n) in two indeterminates satisfies*

$$\psi(m, n) = (1 - q^{-m})f(m, n) + O(mnq^{mn}) + O(q^{m(n+1)}), \tag{4.8}$$

where $f(m, n)$ is the total number of normalized polynomials of degrees (m, n) and the constants implied in the O-terms depend only on q. In particular for fixed m we have

$$\psi(m, n) = (1 - q^{-m})f(m, n) + O(nq^{mn}) \tag{4.9}$$

and

$$\psi(m, n) \sim (1 - q^{-m})f(m, n) \qquad (n \to \infty). \tag{4.10}$$

REFERENCE

1. L. Carlitz, *The distribution of irreducible polynomials in several indeterminates*, Ill. J. Math., 7 (1963), 371–5.

Duke University,
Durham, North Carolina