SOME FORMULAS FOR FACTORABLE POLYNOMIALS IN SEVERAL INDETERMINATES†

BY LEONARD CARLITZ

1. *Introduction.* By a factorable polynomial‡ in the $GF(p^n)$ will be meant a polynomial in the indeterminates $x_1, \cdots, x_k$, which factors into a product of linear factors in some (sufficiently large) Galois field:

$$G \equiv G(x_1, \cdots, x_k) \equiv \prod_{j=1}^{m} (\alpha_{j0} + \alpha_{j1}x_1 + \cdots + \alpha_{jk}x_k).$$

It is frequently convenient to consider separately those G (of degree m) in which x_k^m (or any assigned x_i^m) actually occurs; we use the notation G^* to denote such a polynomial. In the case $k=1$, the polynomials G reduce to ordinary polynomials in a single indeterminate; in this case G and G^* are identical.

In this note we extend certain results§ for $k=1$ to the case $k>1$. For polynomials G^* the extensions may (roughly) be obtained by merely replacing p^n by p^{nk}; for arbitrary G the generalizations are not quite so simple.

2. *The μ-Function.* For G of degree m, we put $|G| = p^{nm}$; then

$$\zeta^*(w) = \sum_{G^*} \frac{1}{|G|^w} = (1 - p^{n(k-w)})^{-1}, \tag{1}$$

$$\begin{aligned} \zeta(w) &= \sum_{G} \frac{1}{|G|^w} \\ &= \left\{(1 - p^{n(1-w)})(1 - p^{n(2-w)}) \cdots (1- p^{n(k-w)})\right\}^{-1}, \end{aligned} \tag{2}$$

the sums extending over *all* G^*, G, respectively.

Let $f(m)$ be the number of (non-associated) G of degree m, $f^*(m)$ the number of G^*; from the first of these formulas it follows that $f^*(m) = p^{nkm}$, and from the second, $f(m) = [k+m-1, m]p^{nm}$, where

† Presented to the Society, December 31, 1936.

‡ Duke Mathematical Journal, vol. 2 (1936), pp. 660–670.

§ American Journal of Mathematics, vol. 54 (1932), pp. 39–50; this Bulletin, vol. 38 (1932), pp. 736–744.

$$(3) \qquad [k, s] = \frac{(p^{kn} - 1)(p^{(k-1)n} - 1) \cdots (p^{(k-s+1)n} - 1)}{(p^n - 1)(p^{2n} - 1) \cdots (p^{sn} - 1)}.$$

Taking the reciprocal of (1) and (2), we have

$$(4) \qquad \sum_{G^*} \frac{\mu(G)}{|G|^w} = 1 - p^{n(k-w)},$$

$$(5) \qquad \sum_{G} \frac{\mu(G)}{|G|^w} = \prod_{j=1}^{k} (1 - p^{n(j-w)}),$$

where $\mu(G)$ is the Möbius function. From (4) it follows that

$$\sum_{\deg G^*=m} \mu(G) = \begin{cases} -p^{nk} \text{ for } m = 1, \\ 0 \quad \text{ for } m > 1; \end{cases}$$

on the other hand, from (5) follows

$$\sum_{\deg G=m} \mu(G) = \begin{cases} (-1)^m [k, m] p^{nm(m+1)/2} & \text{for } m \leqq k, \\ 0 & \text{for } m > k, \end{cases}$$

where $[k, m]$ is defined by (3).

3. *The Divisor Functions.* If $\tau(G)$ denotes the number of divisors of G, then it is clear from (1) that

$$(6) \qquad \sum_{G^*} \frac{\tau(G)}{|G|^w} = (1 - p^{n(k-w)})^{-2},$$

while from (2) it follows that

$$(7) \qquad \sum_{G} \frac{\tau(G)}{|G|^w} = \prod_{j=1}^{k} (1 - p^{n(j-w)})^{-2}.$$

From (6) we have at once

$$\sum_{\deg G^*=m} \tau(G) = (m + 1) p^{nmk}.$$

Similarly by means of (7), we may evaluate $\sum \tau(G)$, summed over all G of degree m:

$$\sum_{\deg G=m} \tau(G) = \sum_{m=i+j} [k + i - 1, i][k + j - i, j] p^{nm}.$$

For the function $\sigma_t(G) = \sum |D|^t$, summed over all divisors of G, there are the formulas

$$(8)\quad \sum_{G} \frac{\sigma_t(G)}{|G|^w} = \zeta(w)\zeta(w-t), \qquad \sum_{G^*} \frac{\sigma_t(G)}{|G|^w} = \zeta^*(w)\zeta^*(w-t).$$

From the latter it is clear that

$$\sum_{\deg G^*=m} \sigma_t(G) = p^{nkm} \frac{p^{nt(m+1)}-1}{p^{nt}-1}.$$

The corresponding formula for $\sum \sigma_t(G)$, summed over *all* G of degree m, is not so simple in general. However, if $t=k$, the product $\zeta(w)\zeta(w-k)$ is itself a zeta-function, and thus we get from the first equation in (8)

$$\sum_{\deg G=m} \sigma_k(G) = [2k+m-1, m]p^{nm}.$$

4. *The ϕ-Functions.* Obviously, the Euler ϕ-function cannot be defined in terms of a reduced residue system. Instead we define $\phi_s(G)$ as the number of polynomials A of degree s such that $(A, G)=1$. For $k=1$, $s=\deg G$, $\phi_s(G)$ reduces to the Euler function (for polynomials in a single indeterminate). From the definition it is easily seen that

$$\sum_{s=0}^{\infty} \phi_s(G)p^{-nsw} = \sum_{(A,G)=1} |A|^{-w} = \zeta(w)\prod_{P|G}(1-|P|^{-w}),$$

and therefore, by equating coefficients of p^{-nsw},

$$(9)\qquad \phi_s(G) = \sum_{D|G}{}' \mu(D)f(s-d),$$

where $d=\deg D$, and the sum is over all divisors of degree $\leqq s$. For $s \geqq \deg G$, the sum is over all D; for $s=\deg G$, we shall omit the subscript, so that

$$(10)\qquad \phi(G) = \sum_{D|G} \mu(D)f(s-d),$$

summed over all divisors of G.

Similarly, $\phi_s^*(G)$ is the number of A^* of degree s such that $(A, G)=1$. Then

$$(11)\quad \phi_s^*(G) = \sum_{D|G}{}' \mu(D)f^*(s-d) = |G|^k \sum_{D|G}{}' \mu(D)|D|^{-k}.$$

Again for $s=\deg G$, we write simply $\phi^*(G)$, and we have

$$(12)\quad \phi^*(G) = |G|^k \sum_{D|G} \mu(D)\,|D|^{-k} = |G|^k \prod_{P|G} (1 - |P|^{-k}),$$

where P denotes a typical irreducible divisor of G.

For $\phi^*(G)$ the sum function (taken over G^*) is quite simple. Substituting from (12), we find

$$(13)\qquad \sum_{G^*} \frac{\phi^*(G)}{G^w} = \sum_{D^*} \frac{\mu(D)}{|D|^w} \sum_{E^*} \frac{|E|^k}{|E|^w} = \frac{\zeta^*(w-k)}{\zeta^*(w)}$$
$$= (1 - p^{n(k-w)}) \sum_{j=0}^{\infty} p^{nj(2k-w)},$$

and therefore

$$(14)\qquad \sum_{\deg G^*=m} \phi^*(G) = p^{2nmk} - p^{nk(2m-1)} \qquad \text{for} \quad m \geqq 1.$$

In the second place, we may extend the sum in the left member of (13) over all G:

$$\sum_{G} \frac{\phi^*(G)}{|G|^w} = \sum_{D} \frac{\mu(D)}{|D|^w} \sum_{E} \frac{|E|^k}{|E|^w} = \frac{\zeta(w-k)}{\zeta(w)},$$

from which follows

$$\sum_{\deg G=m} \phi^*(G) = \sum_{m=i+j} (-1)^i [k, i][k+j-1, j] p^{n(k+1)j} p^{ni(i+1)/2}.$$

For $\phi(G)$ the formulas corresponding to (13) and (14) are

$$(15)\qquad \sum_{G^*} \frac{\phi(G)}{|G|^w} = \sum_{D^*} \frac{\mu(D)}{|D|^w} \sum_{E^*} \frac{f(e)}{|E|^w} = \frac{\zeta(w-k)}{\zeta^*(w)},$$

and

$$\sum_{\deg G^*=m} \phi(G) = [k+m-1, m] p^{nm(k+1)}$$
$$- [k+m-2, m-1] p^{n(mk+m-1)}.$$

Finally, if the sum on the left of (15) be taken over all G,

$$\sum_{G} \frac{\phi(G)}{|G|^w} = \sum_{D} \frac{\mu(D)}{|D|^w} \sum_{E} \frac{f(e)}{|E|^w} = \frac{1}{\zeta(w)} \sum_{e=0}^{\infty} \frac{f^2(e)}{p^{new}},$$

and therefore

$$\sum_{\deg G=m} \phi(G) = \sum_{m=i+j} (-1)^i [k, i][k+j-1, j]^2 p^{ni(i+1)/2} p^{2nj}.$$

We remark that more general ϕ-functions may be defined, and the corresponding sum functions constructed exactly as above. For brevity the formulas are omitted.

5. *The q-Functions.* We now consider polynomials L that are not divisible by the eth power of an irreducible. The number of L of degree m will be denoted by $q_e(m)$; the number of L^* by $q_e^*(m)$. For the latter function, it is evident that

$$\sum_{m=0}^{\infty} q_e^*(m) p^{-nmw} = \prod_{P^*} (1 + |P|^{-w} + \cdots + |P|^{-(e-1)w}) = \frac{\zeta^*(w)}{\zeta^*(ew)},$$

where P^* denotes a typical irreducible starred polynomial. Then

$$q_e^*(m) = \begin{cases} p^{nmk} & \text{for } m < e, \\ p^{nmk} - p^{nk(m-e+1)} & \text{for } m \geqq e. \end{cases} \tag{16}$$

On the other hand, since

$$\sum_{m=0}^{\infty} q_e(m) p^{-nmw} = \frac{\zeta(w)}{\zeta(ew)}$$

$$= \sum_{i=0}^{\infty} [k+i-1, i] p^{ni} p^{-nwi} \sum_{j=0}^{k} (-1)^j [k, j] p^{nj(j+1)/2} p^{-newj},$$

we have in place of (16),

$$q_e(m) = \sum_{m=i+ej} (-1)^j [k+i-1, i][k, j] p^{ni} p^{nj(j+1)/2}. \tag{17}$$

Next, let

$$Q(m) = \prod_{\deg L = m} L, \qquad Q^*(m) = \prod_{\deg L^* = m} L^*.$$

If we put

$$D_s = D_s(x_1, \cdots, x_k) = \left| x_i^{p^{nsj}} \right|, \qquad (i, j = 0, \cdots, k),$$

where x_0 is replaced by 1, and

$$\Delta_s = \frac{D_s(x_1, \cdots, x_k)}{D_s(x_1, \cdots, x_{k-1})},$$

then for

$$F_e^*(m) = \Delta_m \Delta_{m-1}^{p^{nek}} \cdots \Delta_1^{p^{nek(m-1)}},$$

we may show, exactly as in the case† $k=1$, that

$$\prod_{s=0}^{h}\{Q^*(se+r)\}^{p^{nk(h-s)}} = F_1^*(he+r)\{F_e^*(h)\}^{-ep^{nkr}} \tag{18}$$
$$= R_e(he+r),$$

say, where $0 \leqq r < e$. From (18) follows at once

$$Q_e^*(m) = R_e(m)\{R_e(m-e)\}^{-p^{nk}}. \tag{19}$$

For $Q(m)$ the generalization is not entirely satisfactory. In place of (18) we have

$$\prod_{s=0}^{h}\{Q_e(se+r)\}^{f(h-s)} = \frac{F(he+r)}{\prod_{j=0}^{h-1} D_{h-j}^{ef(je+r)}},$$

where

$$F(m) = D_m D_{m-1}^{f(1)} \cdots D_1^{f(m-1)}$$

(the product of all polynomials of degree m). However, there seems to be no simple formula like (19) for $Q_e(m)$.

DUKE UNIVERSITY

† See p. 743 of the paper in this Bulletin referred to above.