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 $x_1, \ldots, x_k$, which factors into a product of linear factors in some (sufficiently large) Galois field:

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

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 $\mu$-Function. For $G$ of degree $m$, we put $|G| = p^{nm}$; then

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

$$\xi(w) = \sum_{G} \frac{1}{|G|^w} = \left\{ (1 - p^{n(1-w)})(1 - p^{n(2-w)}) \cdots (1 - p^{n(k-w)}) \right\}^{-1},$$

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 $f^*(m) = p^{nk_m}$, and from the second, $f(m) = [k + m - 1, m] p^{nm}$, where

---

† Presented to the Society, December 31, 1936.  
Taking the reciprocal of (1) and (2), we have

\begin{equation}
\sum_{G} \frac{\mu(G)}{|G|^w} = 1 - p^{n(k-w)},
\end{equation}

and

\begin{equation}
\sum_{G} \frac{\mu(G)}{|G|^w} = \prod_{j=1}^{k} (1 - p^{n(j-w)}),
\end{equation}

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

\[ \sum_{\deg G = m} \mu(G) = \begin{cases} -p^m k & \text{for } m = 1, \\ 0 & \text{for } m > 1; \end{cases} \]

on the other hand, from (5) follows

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

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

\begin{equation}
\sum_{G} \frac{\tau(G)}{|G|^w} = (1 - p^{n(k-w)})^{-2},
\end{equation}

while from (2) it follows that

\begin{equation}
\sum_{G} \frac{\tau(G)}{|G|^w} = \prod_{j=1}^{k} (1 - p^{n(j-w)})^{-2}.
\end{equation}

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
From the latter it is clear that
\[ \sigma_l(G) = \zeta(w)\zeta(w - t), \quad \sum_{G} \frac{\sigma_l(G)}{|G|^w} = \zeta^*(w)\zeta^*(w - t). \]

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

4. The \( \phi \)-Functions. Obviously, the Euler \( \phi \)-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
\[ \sum_{s=0}^\infty \phi_s(G) p^{-nw} = \sum_{(A, G) = 1} |A|^{-w} = \zeta(w) \prod_{P|G} (1 - |P|^{-w}), \]

and therefore, by equating coefficients of \( p^{-nw} \),
\[ \phi_s(G) = \sum_{D|G} \mu(D) f(s - d), \]

where \( d = \deg D \), and the sum is over all divisors of degree \( \leq s \). For \( s \geq \deg G \), the sum is over all \( D \); for \( s = \deg G \), we shall omit the subscript, so that
\[ \phi(G) = \sum_{D|G} \mu(D) f(s - d), \]

summed over all divisors of \( G \).

Similarly, \( \phi_s^*(G) \) is the number of \( A^* \) of degree \( s \) such that \( (A, G) = 1 \). Then
\[ \phi_s^*(G) = \sum_{D|G} \mu(D) f^*(s - d) = |G|^s \sum_{D|G} \mu(D) |D|^{-b}. \]

Again for \( s = \deg G \), we write simply \( \phi^*(G) \), and we have
(12) \[ \phi^*(G) = |G|^k \sum_{D \mid G} \mu(D) |D|^{-k} = |G|^k \prod_{P \mid G} (1 - |P|^{-k}), \]
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

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

and therefore

\[
(14) \quad \sum_{\text{deg } G^* = m} \phi^*(G) = p_{2nmk} - p_{nk(2m-1)} \quad \text{for } m \geq 1.
\]

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

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

from which follows

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

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

\[
(15) \quad \sum_{G^*} \frac{\phi(G)}{|G|^w} = \sum_{D^*} \frac{\mu(D)}{|D|^w} \sum_{E^*} \frac{f(e)}{|E|_w} = \frac{\zeta(w - k)}{\tilde{\zeta}^*(w)},
\]

and

\[
\sum_{\text{deg } G^* = m} \phi(G) = [k + m - 1, m]p_{nm(k+1)}
\]

\[
- [k + m - 2, m - 1]p_{nm(k+1)}.
\]

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

\[
\sum_{\text{deg } G = m} \phi(G) = \sum_{m=} (-1)^i[k, i][k + j - 1, j]^2p_{n(i+1)/2}p_{2nij}.
\]
We remark that more general \( \phi \)-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 \( e \)th 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

\[
\sum_{m=0}^{\infty} q^*_e(m) p^{-nmw} = \prod_{P^*} \left(1 + | P |^{-w} + \cdots + | P |^{-(e-1)w}\right) = \frac{\zeta^*(w)}{\zeta^*(ew)},
\]

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

\[
q^*_e(m) = \begin{cases} 
  p^{nmk} & \text{for } m < e, \\
  p^{nmk} - p^{nk(m-e+1)} & \text{for } m \geq e.
\end{cases}
\]

On the other hand, since

\[
\sum_{m=0}^{\infty} q_e(m) p^{-nmw} = \frac{\zeta(w)}{\zeta(ew)} = \sum_{i=0}^{\infty} [k + i - 1, i] [k, j] p^{ni} p^{-nw i} \sum_{j=0}^{k} (-1)^j [k, j] p^{nj(i+1)/2} p^{-new j},
\]

we have in place of (16),

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

Next, let

\[
Q(m) = \prod_{\deg L = m} L, \quad Q^*(m) = \prod_{\deg L^* = m} L^*.
\]

If we put

\[
D_s = D_s(x_1, \ldots, x_k) = \left| x_i^{nj} \right|, \quad (i, j = 0, \ldots, k),
\]

where \( x_0 \) is replaced by 1, and

\[
\Delta_s = \frac{D_s(x_1, \ldots, x_k)}{D_s(x_1, \ldots, x_{k-1})},
\]

then for

\[
F^*_e(m) = \Delta_m \Delta_{m-1}^{p^e_k} \cdots \Delta_1^{p^e_k(m-1)},
\]
we may show, exactly as in the case $k = 1$, that

\begin{equation}
\prod_{s=0}^{h} \left\{ Q^*(se + r) \right\}^{\mu_{nk(h-s)}} = R^*(he + r) \left\{ P^*(h) \right\} - \epsilon_{nkhr}
\end{equation}

\begin{equation*}
= R^*(he + r),
\end{equation*}

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

\begin{equation}
Q^*_e(m) = R_e(m) \left\{ R_e(m - e) \right\} - \epsilon_{nkhr}.
\end{equation}

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

\begin{equation*}
\prod_{s=0}^{h} \left\{ Q_e(se + r) \right\}^{f(h-s)} = \frac{F(he + r)}{\prod_{j=0}^{h-1} D_{h-i}^{f(je + r)}},
\end{equation*}

where

\begin{equation*}
F(m) = D_mD_{m-1}^{(3)} \cdots D_1^{(m-1)}
\end{equation*}

(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.