On the Factorization of Some Polynomial Analogues of Binomial Coefficients

By

Carl G. Wagner *)

In [4] Scheid proved that if $1 < k < n - 1$, then $\binom{n}{k}$ is not a power of a prime. He also stated a lower bound for the number of distinct prime divisors of $\binom{n}{k}$. In the present note we prove a similar theorem about the factorization of certain polynomials over a finite field.

Let $GF[q, x]$ denote the ring of polynomials over the finite field $GF(q)$ and let $GF(q, x)$ be the quotient field of $GF[q, x]$. Define a sequence of polynomials $\psi_k(t)$ over $GF[q, x]$ by

$$(1) \qquad \psi_k(t) = \prod_{\deg m < k} (t - m),$$

where the product in (1) is taken over all $m \in GF[q, x]$ (including 0) of degree $< k$. In addition, define a sequence (F_k) in $GF[q, x]$ by

$$(2) \qquad F_k = \langle k \rangle \langle k-1 \rangle^q \langle k-2 \rangle^{q^2} \dots \langle 1 \rangle^{q^{k-1}}, \quad F_0 = 1,$$

where

$$(3) \qquad \langle n \rangle = x^{q^n} - x.$$

Carlitz [2] has proved that the sequence $(\psi_k(t)/F_k)$ is an ordered basis of the $GF[q, x]$-module of linear, integral valued polynomials over $GF(q, x)$. (A polynomial $f(t)$ over $GF(q, x)$ is called *integral valued* if $f(m) \in GF[q, x]$ whenever $m \in GF[q, x]$.) Hence, the polynomials $\psi_k(t)/F_k$ are function field analogues of the Newton polynomials $\binom{t}{n}$, and so the $\psi_k(m)/F_k$, for $m \in GF[q, x]$, may be regarded as polynomial analogues of binomial coefficients. The quantities $\psi_k(m)/F_k$ also occur in connection with the Carlitz ψ-function [1].

The proof of our main theorem is based on the following lemma:

Lemma. *Let $\pi \in GF[q, x]$ be a monic irreducible polynomial. Let*

$$k \geqq 1, \quad m^* \in GF[q, x], \quad \textit{and} \quad \deg m^* > k.$$

*) This work was supported by a grant from the University of Tennessee Faculty Research Fellowship Fund.

Let $m^* = m_0 + m_1\pi + \cdots + m_s\pi^s$ *be the* π*-adic expansion of* m^*. *For*

$$m \in GF[q,x] - \{0\},$$

let $v_\pi(m)$ *be the largest integer* i *for which* $\pi^i | m$. *Then* $v_\pi(\psi_k(m^*)/F_k) \leqq s$.

Proof. Let $\deg \pi = d$ and $\deg m^* = r$. Recall that π divides $\langle n \rangle$ exactly once in $GF[q,x]$ if and only if $d | n$. Hence, by (2) and (3),

$$v_\pi(F_k) = \sum_{j=1}^{[k/d]} q^{k-jd}, \tag{4}$$

where $[k/d]$ is the greatest integer in k/d.

To evaluate $v_\pi(\psi_k(m^*))$, define integers α_j for $j \geqq 1$ by

$$\alpha_j = \operatorname{card}\{m \in GF[q,x] : \deg m < k \quad \text{and} \quad m \equiv m^* (\operatorname{mod} \pi^j)\}. \tag{5}$$

Then

$$v_\pi(\psi_k(m^*)) = \sum_{\deg m < k} v_\pi(m^* - m) = \sum_{j=1}^{\infty} j(\alpha_j - \alpha_{j+1}) = \sum_{j=1}^{\infty} \alpha_j, \tag{6}$$

where, in the last two sums in (6), all but a finite number of terms vanish. To evaluate the α_j, note first that since $k < r$, $\alpha_j = 0$ for $j > s$. For $1 \leqq j \leqq [k/d]$, the set $S_k = \{m \in GF[q,x] : \deg m < k\}$ contains precisely q^{k-jd} complete residue systems $(\operatorname{mod} \pi^j)$ so that $\alpha_j = q^{k-jd}$ for such j. For $[k/d] < j < s$, however, $\alpha_j \leqq 1$, since S_k contains only a fragment of a complete residue system $(\operatorname{mod} \pi^j)$. In view of the preceeding remarks,

$$\begin{aligned} v_\pi(\psi_k(m^*)/F_k) &= v_\pi(\psi_k(m^*)) - v_\pi(F_k) = \\ &= \sum_{j=1}^{[k/d]} \alpha_j + \sum_{j=[k/d]+1}^{s} \alpha_j - \sum_{j=1}^{[k/d]} q^{k-jd} \leqq s, \end{aligned} \tag{7}$$

as desired.

Note. The restriction $\deg m^* > k$ in the above does not exclude any interesting cases, for $\psi_k(m^*) = 0$ if $\deg m^* < k$, and if $\deg m^* = k$, $\psi_k(m^*) = \alpha F_k$, where α is the leading coefficient of m^* [3, p. 140].

Theorem. *Let* $k \geqq 1$, $m \in GF[q,x]$, *and* $\deg m^* = r > k$. *Let* $\pi_1, \pi_2, \ldots, \pi_\omega$ *be the distinct monic irreducible divisors of* $\psi_k(m^*)/F_k$. *Then* $\omega \geqq (r-k)q^k/r$.

Proof. Let $\deg \pi_i = d_i$ and let $m^* = m_0^i + m_1^i \pi_i + \cdots + m_{s_i}^i \pi_i^{s_i}$ be the π_i-adic expansion of m^* for $1 \leqq i \leqq \omega$. It follows that $s_i d_i \leqq r$, and so

$$s_1 d_1 + \cdots + s_\omega d_\omega \leqq r\omega.$$

Suppose that $\psi_k(m^*)/F_k = \lambda \pi_1^{e_1} \cdots \pi_\omega^{e_\omega}$, where $\lambda \in GF(q)$. By the lemma, $e_i \leqq s_i$ for $1 \leqq i \leqq \omega$. Hence,

$$\begin{aligned} \deg \psi_k(m^*)/F_k = (r-k)q^k = e_1 d_1 + \cdots + e_\omega d_\omega &\leqq \\ \leqq s_1 d_1 + \cdots + s_\omega d_\omega &\leqq r\omega, \end{aligned}$$

and $\omega \geqq (r-k)q^k/r$ or, if a cruder estimate not involving r is desired, $\omega \geqq q^k/k + 1$.

Corollary. *Let k and m^* be as in the preceding theorem. Then, unless $q = 2$, $k = 1$, and $r = 2$, $\psi_k(m^*)/F_k$ is not simply a power of an irreducible polynomial.*

Proof. If $q \geqq 3$ and $k \geqq 1$, or if $q = 2$ and $k \geqq 2$, then $q^k > k + 1$ and $\omega \geqq \geqq q^k/k + 1 > 1$. If $q = 2$, $k = 1$, and $r \geqq 3$, then $(r - k)\,q^k > r$ and $\omega \geqq (r - k) \times \times q^k/r > 1$. In the remaining case we have $\psi_1(x^2)/F_1 = \psi_1(x^2 + 1)/F_1 = x(x + 1)$ and, as exceptions to the general rule,

$$\psi_1(x^2 + x)/F_1 = \psi_1(x^2 + x + 1)F_1 = x^2 + x + 1\,.$$

Reference

[1] L. CARLITZ, A class of polynomials. Duke Math. J. **6**, 486—504 (1940).
[2] L. CARLITZ, A set of polynomials. Trans. Amer. Math. Soc. **43**, 167—182 (1938).
[3] L. CARLITZ, On certain functions connected with polynomials in a Galois field. Duke Math. J. **1**, 137—168 (1935).
[4] H. SCHEID, Die Anzahl der Primfaktoren in $\binom{n}{k}$. Arch. Math. **20**, 581—582 (1969).

Eingegangen am 11. 10. 1971

Anschrift des Autors:
Carl G. Wagner
Department of Mathematics
University of Tennessee
Knoxville, Tennessee 37916, USA