BULLETIN
of the
MALAYSIAN MATHEMATICAL SOCIETY

Bull. Malaysian Math. Soc. (Second Series) **22** (1999) 45-52

Multiply Integer-Valued Polynomials in a Galois Field

VICHIAN LAOHAKOSOL AND KANNIKA KONGSAKORN
Department of Mathematics, Kasetsart University, Bangkok 10900, Thailand

Abstract. Consider the elements from the ring $F_q[x]$ of polynomials over a Galois field F_q as integers. A polynomial $f(T)$ over $F_q(x)$ is said to be integer-valued if $f(T)$ takes values in $F_q[x]$ for all T in $F_q[x]$. We derive conditions for a polynomial which together with its higher derivatives are integer-valued.

1. Introduction

Let $F_q[x]$ be the ring of polynomials over the Galois (finite) field F_q of characteristic p with $q = p^n$, and $F_q(x)$ its quotient field. For positive integer m, let

$$[m] = x^{q^m} - x,\ [0] = 0,\ L_m = [m][m-1]\cdots[1],\ L_0 = 1,$$
$$F_m = [m][m-1]^q \cdots [1]^{q^{m-1}},\ F_0 = 1.$$

It is known (Carlitz [1]) that F_m is the product of all monic polynomials in $F_q[x]$ of degree m, and L_m is the least common multiple of all polynomials in $F_q[x]$ of degree m. Define the linear Carlitz polynomials by

$$\psi_0(T) = T,\ \psi_m(T) = \prod_{\deg M < m} (T - M),$$

where the product extends over all polynomials $M \in F_q[x]$, including 0, of degree less than m. The polynomial $\psi_m(T)$ is of degree q^m in T with coefficients in $F_q[x]$. A polynomial $f(T)$ is called **linear** if $f(T+U) = f(T) + f(U),\ f(cT) = cf(T)$ for all $c \in F_q$. From [1], we know that any linear polynomial in $F_q(x)[T]$ of degree q^m has a unique ψ-representation of the form $\sum_{i=0}^{m} A_i\ \psi_i(T)$, $A_i \in F_q(x)$. Write a positive

integer m with respect to base q as $m = \alpha_0 + \alpha_1 q + \cdots + \alpha_s q^s$, where $\alpha_i \in \{0, 1, \cdots, q-1\}$, $\alpha_s \neq 0$. Define the (general) Carlitz polynomials by

$$G_m(T) = \psi_0^{\alpha_0}(T)\,\psi_1^{\alpha_1}(T)\cdots\,\psi_s^{\alpha_s}(T)\,,\quad G_0(T) = 1\,,$$

and let $g_m = F_0^{\alpha_0} F_1^{\alpha_1} \cdots F_s^{\alpha}$, $g_0 = 1$. We know ([3]) that $G_m(T)$ is a polynomial in T of degree m with coefficients in $\mathbb{F}_q[x]$, and any polynomial of degree m in $\mathbb{F}_q(x)[T]$ has a unique G-representation of the form $\sum_{i=0}^{m} A_i G_i(T)$, $A_i \in \mathbb{F}_q(x)$. Define the related Carlitz polynomials $H_m(T)$ of degree m by

$$H_m(T) = \prod_{i=0}^{s} H_{\alpha_i q^i}(T)\,,\ \text{where}\ H_{\alpha q^i}(T) = \begin{cases} \psi_i^{\alpha}(T) & \text{for}\quad 0 \le \alpha \le q-2 \\ \psi_i^{\alpha}(T) - F_i^{\alpha} & \text{for}\quad \alpha = q-1 \end{cases}$$

Note that $H_{q^m-1}(T) = \psi_m(T)/T$. An integer-valued polynomial is a polynomial $f(T) \in \mathbb{F}_q(x)[T]$ such that $f(M) \in \mathbb{F}_q[x]$ for all $M \in \mathbb{F}_q[x]$. Denote by IVP the class of integer-valued polynomials. It is known (Carlitz [3]) that:

(i) a linear polynomial $f(T) = \sum_{i=0}^{m} A_i\,\psi_i(T)$ is integer-valued if and only if $A_i F_i \in \mathbb{F}_q[x]$, i.e. $\psi_i(T)/F_i$ form a basis over $\mathbb{F}_q[x]$ for linear IVP, and

(ii) a polynomial $f(T) = \sum_{i=0}^{m} A_i G_i(T)$ is integer-valued if and only if $A_i g_i \in \mathbb{F}_q[x]$, i.e. $G_i(T)/g_i$ form a basis over $\mathbb{F}_q[x]$ for IVP. In 1948, Carlitz [4] applied the method of interpolation to prove that

(iii) a linear polynomial $f(T)$ of degree q^m is integer-valued if and only if $f(x^j) \in \mathbb{F}_q[x]$ for all $j \in \{1, 2, \cdots, m\}$, and

(iv) a polynomial $f(T)$ of degree less than q^m is integer-valued if and only if $f(M) \in \mathbb{F}_q[x]$ for all $M \in \mathbb{F}_q[x]$ of degree less than m.

Mimicking the proof of (iv) in Carlitz [4] but using instead the interpolation formula (3.9) of Carlitz [3], we have

(iv)' a polynomial $f(T)$ of degree less than q^m is integer-valued if and only if $f(M) \in \mathbb{F}_q[x]$ for all monic $M \in \mathbb{F}_q[x]$ of degree m.

The objective of this paper is to extend these last results by obtaining conditions on the functional values of a polynomial which together with its higher derivatives are integer-valued, called **multiply** integer-valued polynomial. This supplements our earlier investigation [5] where bases for multiply integer-valued polynomials are derived. Let us mention in passing that the case of linear polynomials is trivial because their first derivatives are constant.

2. Technical lemmas

Apart from the notation set out in Section 1, we further need the following notation. For integers $k \geq 0$, $j \geq 1$, set

$$S_{k,0} = 1, \quad S_{k,1} = x + x^q + \cdots + x^{q^k}, \quad S_{k,j} = xS_{k,j-1} + x^q S_{k-1,j-1}^q + \cdots + x^{q^k} S_{0,j-1}^{q^k}.$$

Since F_k is the product of all monic polynomials of degree k in $F_q[x]$, then $\psi_k(x^k) = F_k$; we now derive formulas for higher powers of x.

Lemma 1. *For integers $k \geq 0$, $j \geq 1$, we have $\psi_k(x^{k+j}) = F_k S_{k,j}$.*

Proof. From Theorem 2.2 , p. 141 of Carlitz [2] we know that

$$\psi_k(x^{k+1}) - x\psi_k(x^k) = (x^{q^k} - x)\psi_{k-1}^q(x^k)$$

and so $\psi_k(x^{k+1}) = x F_k + [k]\psi_{k-1}^q(x^k)$. Iterating, we get

$$\psi_k(x^{k+1}) = \sum_{i=0}^{k} x^{q^i} [k]_i F_{k-i}^{q^i},$$

where $[k]_0 = 1, [k]_i = [k][k-1]^q \cdots [k-1+1]^{q^{i-1}}$. Since $[k]_i F_{k-i}^{q^i} = F_k$, direct substitution yields the result for the case $j = 1$. The general case then follows by induction on *j*.

Lemma 2. *Let k be a positive integer with base q-representation $k = \alpha_0 + \alpha_1 q + \cdots + \alpha_m q^m$, $\alpha_i \in \{0, 1, \cdots, q-1\}$, $\alpha_m \neq 0$. Then*

$$H_k'(T) = \sum_{j=0}^{m-1} (-1)^j \binom{k}{q^j} H_{k-q^j}(T)\, g_{q^j-1}.$$

In particular,

$$\left(\frac{\psi_k(T)}{T}\right)' = H'_{q^m-1}(T) = \sum_{j=0}^{m-1}(-1)^{j+1} g_{q^j-1}\psi_j^{q-2}\prod_{\substack{i=0\\ i\neq j}}^{m-1}\left(\psi_i^{q-1}(T)-F_i^{q-1}\right)$$

Proof. From the equation (2.6) p.489 of Carlitz [3], we have

$$\frac{H_k(T+U)-H_k(T)}{U} = \sum_{i=0}^{k-1}\binom{k}{i}H_i(T)\frac{G_{k-i}(U)}{U} .$$

From Proposition 3, p.208 of Wagner [6], we know that

$$\frac{G_n(U)}{Ug_{n-1}}\Big|_{U=0} = \begin{cases}(-1)^k & , \text{ if } n=q^k\\ 0 & , \text{ otherwise}\end{cases}.$$

The first result follows by taking limits and substituting these relations into the sum. The second result follows from the definition of H_k, and the observation that

$$q^m-1-q^i = (q-1)\sum_{\substack{i=0\\ i\neq j}}^{m-1}q^i+(q-2)q^j \quad \text{and} \quad \binom{q^m-1}{q^j} = -1 \text{ in } F_q$$

3. Main results

Theorem 1. *Let* $f \in IVP$ *with* $\deg f < q^m$. *Then* $f' \in IVP$ *if and only if either*

(i) *for all* $A \in F_q[x]$, $\deg A < m$, *we have*

$$\sum_{j=0}^{m-1}\frac{1}{L_j}\prod_{i=0}^{j-1}\left(S_{i,j-i}^{q-1}+S_{i,j-i-1}^{q-1}+\cdots+S_{i,1}^{q-1}\right)\sum{}^{*}\frac{f(M)}{c_{A-M}} \in F_q[x],$$

where the inner sum $\sum^*$ *extends over* $M \in F_q[x]$ *such that* $A-M = c_{A-M}x^j +$ *lower powers,* $c_{A-M} \in F_q - \{0\}$, *or*

(ii) *for all monic* $A \in F_q[x]$, $\deg A = m$, *we have*

$$\sum_{j=0}^{m-1} \frac{1}{L_j} \prod_{i=0}^{j-1} \left(S_{i,j-i}^{q-1} + S_{i,j-i-1}^{q-1} + \cdots + S_{i,1}^{q-1} \right) \sum^{**} \frac{f(M)}{c_{A-M}} \in F_q[x],$$

where the inner sum $\sum^{**}$ *extends over monic* $M \in F_q[x]$, $\deg M = m$.

Proof. Since $\deg f < q^m$, then $\deg f' < q^m$ and applying to f' the result (iv) of Carlitz [4] mentioned in the introduction, we get

$$f' \in IVP \Leftrightarrow f'(A) \in F_q[x], \text{ for all } A \in F_q[x], \text{ with } \deg A < m.$$

By the Lagrange interpolation formula (see e.g. (7.1) p. 1009 of Carlitz [4]), noting that when $\deg M < m$, $\psi_m(T) = \psi_m(T - M)$, we have

$$(-1)^m \frac{F_m}{L_m} f(T) = \sum_{\deg M < m} \frac{\psi_m(T)}{T - M} f(M) = \sum_{\deg M < m} \frac{\psi_m(T - M)}{T - M} f(M)$$

$$= \sum_{\deg M < m} H_{q^m - 1}(T - M) \; f(M)$$

and so by Lemma 2,

$$(-1)^m \frac{F_m}{L_m} f'(T) = \sum_{\deg M < m} f(M) \sum_{j=0}^{m-1} (-1)^{j+1} g_{q^j - 1} \psi_j^{q-2}(T - M)$$

$$\prod_{\substack{i=0 \\ i \neq j}}^{m-1} (\psi_i^{q-1}(T - M) - F_i^{q-1})$$

Substituting $T = A$ where $A \in F_q[x]$, $\deg A < m$, we see that the terms with $\deg(A - M) = i \neq j$ drop out because $\psi_i^{q-1}(A - M) = F_i^{q-1}$. Thus the expression on the right hand side becomes, using also Lemma 1,

$$\sum_{j=0}^{m-1} (-1)^{j+1} g_{q^j - 1} \sum^{*} f(M) \frac{(F_0 \cdots F_{m-1})^{q-1}}{F_j c_{A-M}} (-1)^{m-1-j}$$

$$\prod_{i=0}^{j-1} (S_{i,j-i}^{q-1} + S_{i,j-i-1}^{q-1} + \ldots + S_{i,1}^{q-1})$$

Replacing $\frac{g_{q^j-1}}{F_j} = \frac{1}{L_j}$, $(F_0 \cdots F_{m-1})^{q-1} = \frac{F_m}{L_m}$ and cancelling like terms the desired result follows. For the proof of (ii), we start, instead, from the result (iv)' mentioned in the introduction and the Lagrange interpolation formula (see. (3.3), (3.5), and (3.9), pp. 490-492, of Carlitz[3])

$$(-1)^m \frac{F_m}{L_m} f(T) = \sum{}^{**} \left(\frac{\psi_m(T-M)}{T-M} \right) f(M),$$

and proceed in the same manner as before.

Remarks. It is clear from the above theorem that similar necessary and sufficient conditions can be derived for integer-valued polynomials of higher orders. Although Theorem 1 provides necessary and sufficient conditions for polynomials to be multiply integer-valued, the conditions so derived are not so easy to use. It is thus desirable to derive simpler, yet only sufficient, condition(s). Indeed, as seen from the proof of the theorem, one such sufficient condition is that $f(M)$ is divisible by F_m/L_m for all M in $\mathbb{F}_q[x]$, with $\deg M < m$. However, we can do better as in the next theorem.

Theorem 2. *Let* $f \in IVP$ *with* $\deg f < q^m$. *If* $F_{m-1} \mid f(M)$ *for all* $M \in \mathbb{F}_q[x]$, $\deg M < m$, *then* $f' \in IVP$.

Proof. Since, see e.g. p. 1010 of [4],

$$\frac{\psi_m(T-M)}{T-M} = \left(\psi_{m-1}^{q-1}(T-M) - F_{m-1}^{q-1}\right) \cdots \left(\psi_0^{q-1}(T-M) - F_0^{q-1}\right)$$

using the fact that $\psi_j'(T) = (-1)^j F_j/L_j$, see e.g. p. 16 of [5], we get

$$\left(\frac{\psi_m(T-M)}{T-M} \right)' = (-1)^m \frac{F_{m-1}}{L_{m-1}} \psi_{m-1}^{q-2}(T-M) \left(\psi_{m-2}^{q-1}(T-M) - F_{m-2}^{q-1}\right) \cdots$$

$$\left(\psi_0^{q-1}(T-M) - F_0^{q-1}\right) + \cdots + (-1)^{j+1} \frac{F_j}{L_j} \left(\psi_{m-1}^{q-1}(T-M) - F_{m-1}^{q-1}\right) \cdots \psi_j^{q-2}(T-M) \cdots$$

$$\left(\psi_0^{q-1}(T-M) - F_0^{q-1}\right) + \cdots + (-1) \frac{F_0}{L_0} \left(\psi_{m-1}^{q-1}(T-M) - F_{m-1}^{q-1}\right) \cdots$$

$$\left(\psi_1^{q-1}(T-M) - F_1^{q-1}\right) \psi_0^{q-2}(T-M).$$

Substituting this expression into the Lagrange interpolation formula, displayed in the proof of Theorem 1, we arrive at

$$(-1)^m \frac{F_m}{L_m} f'(T) = \sum_{\deg M < m} f(M) \sum_{j=0}^{m-1} (-1)^{j+1} \frac{F_j}{L_j} \psi_j^{q-2} (T - M)$$

$$\prod_{\substack{i=0 \\ i \neq j}}^{m-1} (\psi_i^{q-1}(T - M) - F_i^{q-1}).$$

Replacing $\frac{F_j}{L_j} \frac{L_m}{F_m} = \frac{1}{F_{m-1}^{q-1} \cdots F_j^{q-1}}$ and simplifying, we get

$$(-1)^m f'(T) = \sum_{\deg M < m} f(M) \sum_{j=0}^{m-1} (-1)^{j+1} \frac{1}{F_j} \prod_{i=j+1}^{m-1} \left\{ \left(\frac{\psi_i(T-M)}{F_i} \right)^{q-1} - 1 \right\}$$

$$\prod_{i=0}^{j-1} \left(\psi_i^{q-1} (T - M) - F_i^{q-1} \right)$$

The result now follows by noting that ψ_i / F_i is integer-valued.

Immediate from Theorem 2 is the following corollary.

Corollary. *Let* $f \in IVP$ *with* $\deg f < q^m$. *If* $F_{m-1} \cdots F_{m-s} \mid f(M)$ *for all* $M \in \mathbb{F}_q[x]$, $\deg M < m$, *then* $f', \cdots, f^{(s)} \in IVP$.

Remarks. Since, see e.g. [5], any integer-valued polynomial of degree less than q is of the form $f(T) = \sum_{i=0}^{q-1} A_i G_i(T) / g_i \quad (A_i \in \mathbb{F}_q[x]); \; G_i(T) = T^i, \; g_i = 1$ $(i = 0, 1, \cdots, q-1)$, then $f'(T) \in IVP$ automatically showing that Theorem 2 is also necessary when $m = 1$. However for cases of larger *m*, this is far from being true. We illustrate here only the case $m = 2$ where by taking for example $f(T) = \psi_1(T)/F_1 \in IVP$, we get $f'(T) = -1/L_1$ which is certainly not integer-valued.

References

1. L. Carlitz, On polynomials in a Galois field, *Bull. Amer. Math. Soc*. **38** (1932), 736-644.
2. L. Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935), 137-168.
3. L. Carlitz, A set of polynomials, *Duke Math. J.* **6** (1940), 486-504.
4. L. Carlitz, Finite sums and interpolation formulas over $GF[p^n, x]$, *Duke Math. J.* **15** (1948), 1001-1012.
5. V. Laohakosol, Bases for integer-valued polynomials in a Galois field, *Acta Arith. LXXXVII.* **1** (1998), 13-26.
6. C.G. Wagner, Interpolation series in local fields of prime characteristic, *Duke Math. J.* **39** (1972), 203-210.

Keywords and phrases: multiply integer-valued polynomial, Galois field.

AMS Subject Classification: 11T55, 11T06, 11C08, 13F20