ACTA ARITHMETICA
LXXXVII.1 (1998)

Bases for integer-valued polynomials in a Galois field

by

VICHIAN LAOHAKOSOL (Bangkok)

1. Introduction. It is well known (see e.g. Pólya and Szegő [11, Chapter 2]) that $\binom{x}{i}$, $i = 0, 1, 2, \ldots$, is a basis over $\mathbb{Z}$ for the integer-valued polynomials. In 1951, Straus [12] proved that a basis over $\mathbb{Z}$ for the polynomials which together with all their derivatives are rational integral at all rational integers is given by $\prod_p p^{[i/p]}\binom{x}{i}$, $i = 0, 1, 2, \ldots$, where the product runs over all rational primes p. In 1955, de Bruijn [7] (see also Hall [8]) proved that a basis over $\mathbb{Z}$ for the polynomials which together with all their first order differences are rational integral at rational integers is given by $\ell_i\binom{x}{i}$, $i = 0, 1, 2, \ldots$, where ℓ_i denotes the least common multiple of $1, 2, \ldots, i$ and $\ell_0 = 1$.

In 1959, Carlitz [5] proved among other things that a basis over $\mathbb{Z}$ for the polynomials which together with their differences up to order r are rational integral at rational integers is given by $L_i^{(r)}\binom{x}{i}$, $i = 0, 1, 2, \ldots$, where $L_0^{(r)} = 1$ and $L_i^{(r)}$ denotes the least common multiple of the products $s_1 \ldots s_k$ where $s_1, \ldots, s_k$ are positive integers subject to $s_1 + \ldots + s_k \le i$ for all $k = 1, \ldots, r$. Carlitz in the same paper also showed that the class of polynomials which, together with their derivatives of all orders, are rational integral at rational integers coincides with the class of polynomials which, together with all their differences of all orders, are rational integral at rational integers (see also Laohakosol and Ubolsri [9]).

In 1976, Brizolis and Straus [1] proved that a basis over $\mathbb{Z}$ for the doubly integer-valued polynomials, i.e. polynomials which together with their first derivatives take rational integral values at all rational integers, is given by

$$\prod_p p^{k(p,i)}\binom{x}{i} + \sum_{j=1}^{i} a_j^{(i)}\binom{x}{i}, \qquad i = 0, 1, 2, \ldots,$$

where $k(p, i)$ is the greatest integer k such that $kp^k - (k-1)p^{k-1} \le i$, and $a_j^{(i)}$

1991 *Mathematics Subject Classification*: 11T55, 11T06, 11C08, 13F20.
Key words and phrases: integer-valued polynomials, Galois field.

are computable integers. Brizolis and Straus have remarked that there does not exist a basis over $\mathbb{Z}$ for the class of doubly integer-valued polynomials which consists of integral multiples of the polynomials $\binom{x}{i}$ as in other cases mentioned.

In this paper, we consider analogous problems in the polynomial ring $\mathrm{GF}(q,x)[T]$, i.e. the ring of polynomials with coefficients from the rational function field $\mathrm{GF}(q,x)$. This problem was posed in Narkiewicz [10]. In Section 2, we compile the terminology and basic properties that will be used throughout. In Section 3, we state a lemma which will be applied later, as well as briefly collect results about the problems we consider that are known to us. Section 4 treats the case of linear polynomials, which is simpler and where the desired bases can be completely constructed. Section 5 treats the general case; as will be seen our discussion is more or less complete, save only that bases for the cases of higher order derivatives are not explicitly exhibited because the computation involved becomes too messy, but the ideas used for such construction work generally. The messy shape of such bases reflects close similarity with the classical case of doubly integer-valued polynomials mentioned in Brizolis and Straus [1].

2. Preliminaries. The notation and auxiliary results in this section follow closely those in Carlitz [2], [3] and will be kept throughout the paper. Let $\mathrm{GF}[q,x]$ be the ring of polynomials over the Galois (finite) field $\mathrm{GF}(q)$ of characteristic p with $q=p^n$, and $\mathrm{GF}(q,x)$ its quotient field. For positive integer m, let

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

It is known that F_m is the product of all monic polynomials in $\mathrm{GF}[q,x]$ of degree m, and L_m is the least common multiple of all polynomials in $\mathrm{GF}[q,x]$ of degree m. Define a sequence of polynomials over $\mathrm{GF}[q,x]$ by

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

where the product extends over all polynomials $M\in\mathrm{GF}[q,x]$, including 0, of degree less than m. We know that $\psi_m(T)$ is a polynomial in T of degree q^m with coefficients in $\mathrm{GF}[q,x]$ and enjoys the following properties:

$$\psi_m(T)=c\psi_m(T)\quad(\forall c\in\mathrm{GF}(q)),\qquad \psi_m(T+U)=\psi_m(T)+\psi_m(U),$$
$$\psi_m(E)=0\qquad\text{for all } E\in\mathrm{GF}[q,x] \text{ of degree less than } m,$$
$$\psi_m(M)=F_m\qquad\text{for all monic } M\in\mathrm{GF}[q,x] \text{ of degree } m.$$

Note that the first two properties are referred to as linear properties, which is defined as follows: a polynomial $f(T)$ is called *linear* if

$$f(T+U) = f(T) + f(U), \qquad f(cT) = cf(T) \qquad (\forall c \in \mathrm{GF}(q)).$$

It has been shown that any linear polynomial in $\mathrm{GF}(q,x)[T]$ of degree q^m has a unique ψ-representation of the form $\sum_{i=0}^{m} A_i\psi_i(T)$, $A_i \in \mathrm{GF}(q,x)$.

Write a positive integer m with respect to base q as

$$m = \alpha_0 + \alpha_1 q + \ldots + \alpha_s q^s, \qquad \alpha_i \in \{0,1,\ldots,q-1\},\ \alpha_s \neq 0.$$

Define a sequence of (Carlitz) polynomials $\mathrm{GF}[q,x]$ by

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

and let

$$g_m = F_0^{\alpha_0}F_1^{\alpha_1}\ldots F_s^{\alpha_s}, \qquad g_0 = 1.$$

We know that $G_m(T)$ is a polynomial in T of degree m with coefficients in $\mathrm{GF}[q,x]$, and any polynomial of degree m in $\mathrm{GF}(q,x)[T]$ has a unique G-representation of the form (see also Wagner [14], [15])

$$\sum_{i=0}^{m} A_i G_i(T), \qquad A_i \in \mathrm{GF}(q,x).$$

Another related polynomial $G'_m(T)$ of degree m is defined by

$$G'_m(T) = \prod_{i=0}^{s} G'_{\alpha_i q^i}(T),$$

where

$$G'_{\alpha q^i}(T) = \begin{cases} \psi_i^{\alpha}(T) & \text{for } 0 \le \alpha \le q-2, \\ \psi_i^{\alpha}(T) - F_i^{\alpha} & \text{for } \alpha = q-1. \end{cases}$$

An *integer-valued polynomial* is a polynomial $f(T) \in \mathrm{GF}(q,x)[T]$ such that $f(M) \in \mathrm{GF}[q,x]$ for all $M \in \mathrm{GF}[q,x]$. Denote by IVP the class of integer-valued polynomials; by D^r, $r \in \mathbb{N}$, respectively D^∞, the class of integer-valued polynomials which together with their derivatives up to order r, respectively of all orders, are integer-valued, i.e. belong to $\mathrm{GF}[q,x]$.

Let $M_1,\ldots,M_r$ be nonzero elements of $\mathrm{GF}[q,x]$. Define the zeroth difference of f by

$$\Delta^0 f(T) = f(T),$$

the first difference of f by

$$\Delta f(T) = \frac{f(T+M_1) - f(T)}{M_1} \qquad \text{for all choices of } M_1 \in \mathrm{GF}[q,x],$$

and in general, for $r \in \mathbb{N}$, define the rth difference of f by

$$\Delta^r f(T) = \frac{\Delta^{r-1} f(T+M_r) - \Delta^{r-1} f(T)}{M_r} \qquad \text{for all choices of } M_1,\ldots,M_r \in \mathrm{GF}[q,x].$$

Denote by Δ^r, $r \in \mathbb{N}$, respectively Δ^∞, the class of integer-valued polynomials which together with their differences up to order r, respectively of all orders, are integer-valued. We note in passing that the sets IVP, D^r, D^∞, Δ^r, Δ^∞ are all closed under addition and multiplication by elements from $\mathrm{GF}[q,x]$. Throughout, we will find it convenient to make use of the notion of the *q-indices* of a nonnegative integer m. Let the base-q representation of m be $m = \alpha_0 + \alpha_1 q + \ldots + \alpha_{e(m)} q^{e(m)} + \ldots + \alpha_{d(m)} q^{d(m)}$, where $\alpha_i \in \{0, \ldots, q-1\}$, $\alpha_1 = \ldots = \alpha_{e(m)-1} = 0$, $\alpha_{e(m)} \neq 0$, $\alpha_{d(m)} \neq 0$. Then $e(m)$ and $d(m)$ are called the *lower* and *upper q-indices*, respectively, of m. The word *integral* refers to being an element of $\mathrm{GF}[q,x]$.

3. A lemma and known results

LEMMA. (a) *For nonnegative integer i, we have*

$$D\psi_i(T) = (-1)^i \frac{F_i}{L_i} \qquad \left(D := \frac{d}{dT}\right).$$

(b) *For a nonnegative integer $i = \alpha_0 + \alpha_1 q + \ldots + \alpha_s q^s$, we have*

$$D\left(\frac{G_i(T)}{g_i}\right) = \sum_{j=0}^{s} \frac{(-1)^j \alpha_j G_{i-q^j}(T)}{L_j g_{i-q^j}}.$$

(c) *For positive integers $i \geq j$ with base-q $(= p^n)$ representations $i = \alpha_0 + \alpha_1 q + \ldots + \alpha_s q^s$ and $j = \beta_0 + \beta_1 q + \ldots + \beta_s q^s$, we have*

$$\binom{i}{j} \equiv \binom{\alpha_0}{\beta_0}\binom{\alpha_1}{\beta_1} \cdots \binom{\alpha_s}{\beta_s} \pmod{p},$$

where $\binom{\alpha}{0}$ is interpreted as 1.

Proof. For (a), see Wagner [13], and (b) is immediate from (a). For (c), see Comtet [6, p. 9].

Results related to integer-valued polynomials $\mathrm{GF}[q,x]$ available to us are as follows:

1 (Carlitz [3]). *A linear polynomial $f(T) = \sum_{i=0}^{m} A_i \psi_i(T)$ is integer-valued if and only if $A_i F_i \in \mathrm{GF}[q,x]$, i.e. $\psi_i(T)/F_i$ form a basis over $\mathrm{GF}[q,x]$ for linear integer-valued polynomials.*

2 (Wagner [16]). *A linear integer-valued polynomial*

$$f(T) = \sum_{i=0}^{m} \frac{A_i \psi_i(T)}{F_i} \in \Delta(T) \Leftrightarrow L_i \mid A_i,$$

i.e. $L_i \psi_i / F_i$ form a basis over $\mathrm{GF}[q,x]$ for Δ^1.

3 (Carlitz [3]). *A polynomial* $f(T)=\sum_{i=0}^{m} A_i G_i(T)$ *is integer-valued if and only if* $A_i g_i \in \mathrm{GF}[q,x]$, *i.e.* $G_i(T)/g_i$ *form a basis over* $\mathrm{GF}[q,x]$ *for* IVP.

4 (Carlitz [4]). *A linear polynomial* $f(T)$ *of degree* q^m *is integer-valued if and only if* $f(x^j)\in \mathrm{GF}[q,x]$ *for all* $j\in\{1,\ldots,m\}$.

5 (Carlitz [4]). *A polynomial* $f(T)$ *of degree less than* q^m *is integer-valued if and only if* $f(M)\in\mathrm{GF}[q,x]$ *for all* $M\in\mathrm{GF}[q,x]$ *of degree less than* m.

6 (Wagner [17]). *Let* $f(T)=\sum_{i=0}^{m}\frac{A_i G_i(T)}{g_i}\in \mathrm{IVP}$. *Then*

$$f\in\Delta^1 \Leftrightarrow L_{e^*(j)}\mid A_j\ (\forall j\ge 1),\ \textit{where}\ e^*(j)=\max\{e(i):1\le i\le j\},\quad e(i)=\max\{k:q^k\mid i\}. \tag{6.1}$$

$$f\in\Delta^r \Leftrightarrow \overline{L}_j^{(r)}\mid A_j\ (\forall j\ge 1),\ \textit{where}$$
$$\overline{L}_j^{(r)}=\mathrm{lcm}\{L_j^{(s)}:1\le s\le r\},$$
$$L_j^{(r)}=\mathrm{lcm}\{L_{e(i_1)}\ldots L_{e(i_r)}:i_1,\ldots,i_r>0, i_1+\ldots+i_r\le j,\ j!/(i_1!\ldots i_r!(j-i_1-\ldots-i_r)!)\ \textit{is prime to}\ p\}. \tag{6.2}$$

In passing, let us mention two interesting results which can be proved directly:

(i) $L_i\psi_i(T)/TF_i\in\mathrm{IVP}$.

(ii) *The set* $\{L_{e(i)}G_i(T)/Tg_i : i=1,2,\ldots\}$ *forms a basis over* $\mathrm{GF}[q,x]$ *for* IVP.

4. The linear case. As mentioned earlier, Wagner [16] proved

PROPOSITION 1. *The set* $\{L_i\psi_i(T)/F_i : i=0,1,2,\ldots\}$ *forms a basis for linear polynomials belonging to* Δ^1 *over* $\mathrm{GF}[q,x]$.

Since $\Delta^2(L_i\psi_i(T)/F_i)=0$, an immediate consequence of Proposition 1 is

COROLLARY 1. *Every linear polynomial belonging to* Δ^1 *also belongs to* Δ^r *for all* $r\ge 2$.

For the case of derivatives, we now prove the following result.

THEOREM 1. *The set*

$$\left\{\frac{\psi_0(T)}{F_0}, (-1)^i\left(\frac{\psi_{i-1}(T)}{F_{i-1}}+\frac{\psi_i(T)}{F_{i-1}^q}\right) : i=1,2,\ldots\right\}$$

forms a basis for linear polynomials belonging to D^1 *over* $\mathrm{GF}[q,x]$.

Proof. We first show that each basis element has integral derivative. This is evident because $D(\psi_0(T)/F_0)=1/L_0=1$ and $D(\psi_{i-1}(T)/F_{i-1}+\psi_i(T)/F_{i-1}^q)=0$, by part (a) of the Lemma.

Next, let $f(T) = \sum_{i=0}^{m} A_i\psi_i(T)/F_i \in D^1$. To complete the proof, we show that $f(T)$ can be written in the exhibited basis. Since

$$Df(T) = \sum_{i=0}^{m} \frac{(-1)^i A_i}{L_i} \in \mathrm{IVP},$$

multiplying by L_{m-1}, we deduce that $(-1)^m A_m/[m]$ is integral, i.e.

$$A_m = (-1)^m [m] a_m \quad \text{for some } a_m \in \mathrm{GF}[q, x].$$

Thus

$$Df(T) = \sum_{i=0}^{m-2} \frac{(-1)^i A_i}{L_i} + \frac{(-1)^{m-1} A_{m-1} + a_m}{L_{m-1}}.$$

Multiplying by L_{m-2}, we deduce that $((-1)^{m-1} A_{m-1} + a_m)/[m-1]$ is integral, i.e.

$$A_{m-1} = (-1)^m a_m + (-1)^{m-1}[m-1] a_{m-1} \quad \text{for some } a_{m-1} \in \mathrm{GF}[q, x].$$

Continuing in this manner, we have

$$A_i = (-1)^{i+1} a_{i+1} + (-1)^i [i] a_i \quad (i = 0, 1, \ldots, m),$$

where $a_0, a_1, \ldots, a_m, a_{m+1} = 0$ are all in $\mathrm{GF}[q, x]$. Thus

$$\begin{aligned} f(T) &= \sum_{i=0}^{m} ((-1)^{i+1} a_{i+1} + (-1)^i [i] a_i) \frac{\psi_i(T)}{F_i} \\ &= \frac{a_0 \psi_0(T)}{F_0} + \sum_{i=1}^{m} (-1)^i a_i \left(\frac{\psi_{i-1}(T)}{F_{i-1}} + \frac{\psi_i(T)}{F_{i-1}^q} \right), \end{aligned}$$

which completes the proof of Theorem 1.

Since

$$D^2\left(\frac{\psi_0(T)}{F_0}\right) = D^2\left(\frac{\psi_{i+1}(T)}{F_i^q} + \frac{\psi_i(T)}{F_i}\right) = 0,$$

we have

Corollary 2. *Every linear polynomial in D^1 also belongs to $D^r(T)$ for all $r \geq 2$.*

Remarks. It will be shown later that, generally, for each finite positive integer r, we have $\Delta^r \subset D^r$ but $\Delta^\infty = D^\infty$. Generally, however, $\Delta^r \neq D^r$ as shown by the following example in the case $r = 1$. Let

$$\begin{aligned} f(T) &= \frac{\psi_0(T)}{F_0} + \left(\frac{\psi_1(T)}{F_0^q} + \frac{\psi_0(T)}{F_0}\right) + \left(\frac{\psi_2(T)}{F_1^q} + \frac{\psi_1(T)}{F_1}\right) \\ &= \frac{2\psi_0(T)}{F_0} + (1 + [1]) \frac{\psi_1(T)}{F_1} + [2] \frac{\psi_2(T)}{F_2}. \end{aligned}$$

Clearly, $f \in D^1$, but $f \notin \Delta^1$ for $L_1 = [1] \nmid (1 + [1])$, and $L_2 = [2][1] \nmid [2]$.

5. The general case

Definition. Let k and r be positive integers. Define

$$L^{(1)}_{e(k)} = \operatorname{lcm}\big\{L_{e(k-j)} : j \in \mathbb{Z},\ 0 \le j < k, \tbinom{k}{j} \not\equiv 0 \pmod p\big\}$$

$$\text{(note } L^{(1)}_{e(k)} = L_{d(k)}\text{)},$$

$$L^{(2)}_{e(k)} = \operatorname{lcm}\big\{L_{e(k-j_1)} L_{e(j_1-j_2)} : j_1, j_2 \in \mathbb{Z},\ 0 \le j_2 < j_1 < k, \tbinom{k}{j_1}\tbinom{j_1}{j_2} \not\equiv 0 \pmod p\big\},$$

$$L^{(r)}_{e(k)} = \operatorname{lcm}\big\{L_{e(k-j_1)} L_{e(j_1-j_2)} \ldots L_{e(j_{r-1}-j_r)} : j_1, \ldots, j_r \in \mathbb{Z},\ 0 \le j_r < j_{r-1} < \ldots < j_1 < k, \tbinom{k}{j_1}\tbinom{j_1}{j_2} \ldots \tbinom{j_{r-1}}{j_r} \not\equiv 0 \pmod p\big\}, \ldots,$$

$$L^{(\infty)}_{e(k)} = \operatorname{lcm}\big\{L_{e(k-j_1)} L_{e(j_1-j_2)} \ldots : j_1, j_2, \ldots \in \mathbb{Z},\ 0 \le \ldots < j_2 < j_1 < k, \tbinom{k}{j_1}\tbinom{j_1}{j_2} \ldots \not\equiv 0 \pmod p\big\},$$

$$L^{*(r)}_{e(k)} = \operatorname{lcm}\{L^{(1)}_{e(k)}, \ldots, L^{(r)}_{e(k)}\}, \qquad L^{*(\infty)}_{e(k)} = \operatorname{lcm}\{L^{(1)}_{e(k)}, L^{(2)}_{e(k)}, \ldots, L^{(\infty)}_{e(k)}\}.$$

As mentioned earlier, Wagner [17] proved the following two results using slightly different notations.

Proposition 2. *The set* $\{1, L_{d(i)} G_i(T)/g_i : i = 1, 2, \ldots\}$ *forms a basis for* Δ^1 *over* $\mathrm{GF}[q, x]$.

Proposition 3. *The set* $\{1, L^{*(r)}_{e(i)} G_i(T)/g_i : i = 1, 2, \ldots\}$ *forms a basis for* Δ^r *over* $\mathrm{GF}[q, x]$.

An immediate consequence of Proposition 3 is

Corollary 3. *The set* $\{1, L^{*(\infty)}_{e(i)} G_i(T)/g_i : i = 1, 2, \ldots\}$ *forms a basis for* Δ^∞ *over* $\mathrm{GF}[q, x]$.

For the case of derivatives, we prove the following results.

Theorem 2. *The set*

$$\bigg\{1, (-1)^j \bigg(\frac{[j] G_{i+q^j}(T)}{\alpha^{(i+q^j)}_j g_{i+q^j}} + \frac{G_{i+q^{j-1}}(T)\delta(i, q^j - q^{j-1} - 1)}{\alpha^{(i+q^{j-1})}_{j-1} g_{i+q^{j-1}}}\bigg) : j = 0, 1, 2, \ldots;\ i = 0, 1, \ldots, q^{j+1} - q^j - 1\bigg\}$$

where $\alpha^{(k)}_j$ *denotes the* j*th digit in the base-*q *representation of* k, *i.e.*

$$k = \alpha^{(k)}_0 + \alpha^{(k)}_1 q + \ldots + \alpha^{(k)}_{d(k)} q^{d(k)},$$

and

$$\delta(i, q^j - q^{j-1} - 1) = \begin{cases} 1 & \text{if } i = 0, 1, \ldots, q^j - q^{j-1} - 1, \\ 0 & \text{if } i = q^j - q^{j-1}, \ldots, q^{j+1} - q^j - 1 \end{cases}$$

forms a basis for D^1 *over* $\mathrm{GF}[q,x]$, *provided those terms with* $\alpha_j^{(k)} \equiv 0 \pmod p$ *in the denominators are interpreted as* 0.

Proof. Let $f(T) = \sum_{i=0}^{m} A_i G_i(T)/g_i \in \mathrm{IVP}$. By part (b) of our Lemma,

$$\begin{aligned} Df(T) &= \sum_{i=1}^{m} A_i \sum_{j=0}^{d(i)} \frac{(-1)^j \alpha_j^{(i)} G_{i-q^j}(T)}{L_j g_{i-q^j}} \\ &= \sum_{i=0}^{m-1} \left\{ \sum_{j=0}^{d(m-i)} \frac{(-1)^j \alpha_j^{(i+q^j)} A_{i+q^j}}{L_j} \right\} \frac{G_i(T)}{g_i} \\ &= \sum_{i=0}^{m-1} \frac{F(d(m-i)) G_i(T)}{g_i}, \end{aligned}$$

where

$$F(d(m-i)) = \sum_{i=0}^{d(m-i)} \frac{(-1)^j \alpha_j^{(i+q^j)} A_{i+q^j}}{L_j},$$

and $d(i)$ denotes the upper q-index of i. Therefore,

$$Df \in \mathrm{IVP} \Rightarrow F(d(m-i)) \in \mathrm{GF}[q,x] \quad (i = 0, \ldots, m-1).$$

Suppose that $f \in D^1$, and put $c = d(m-i)$, for short. Multiplying $F(c) = F(d(m-i)) \in \mathrm{GF}[q,x]$ by L_{c-1}, we deduce that

$$(-1)^c \alpha_c^{(i+q^c)} A_{i+q^c} = [c] a_{i+q^c} \quad \text{for some } a_{i+q^c} \in \mathrm{GF}[q,x];$$

if $\alpha_c^{(i+q^c)} \equiv 0 \pmod p$, take $a_{i+q^c} = 0$. Multiplying by L_{c-2} to get

$$F(c) = F(c-2) + \frac{(-1)^{c-1} \alpha_{c-1}^{(i+q^{c-1})} A_{i+q^{c-1}} + a_{i+q^c}}{L_{c-1}} \in \mathrm{GF}[q,x],$$

we deduce that

$$(-1)^{c-1} \alpha_{c-1}^{(i+q^{c-1})} A_{i+q^{c-1}} = [c-1] a_{i+q^{c-1}} - a_{i+q^c} \quad \text{for some } a_{i+q^{c-1}} \in \mathrm{GF}[q,x].$$

Continuing in this manner, we arrive at

$$(-1)^j \alpha_j^{(i+q^j)} A_{i+q^j} = [j] a_{i+q^j} - a_{i+q^{j+1}} \qquad (i = 0, \ldots, m-1;\ j = 0, \ldots, d(m-i)),$$

where all $a_{i+q^j} \in \mathrm{GF}[q,x]$, $a_{i+q^{d(m)+1}} = 0$, and $a_{i+q^j} = a_{i+q^{j+1}}/[j]$ if $\alpha_j^{(i+q^j)} = 0$. By adding appropriate zero coefficients at the end if necessary, we can write

$$f(T)=A_0+\sum_{j=0}^{d(m)}\sum_{i=0}^{q^{j+1}-q^j-1}\frac{A_{i+q^j}G_{i+q^j}(T)}{g_{i+q^j}}.$$

Direct substitution yields, provided terms with the α's $\equiv 0 \pmod p$ are taken as 0,

$$f(T)=A_0+\sum_{j=0}^{d(m)}\sum_{i=0}^{q^{j+1}-q^j-1}(-1)^j\frac{[j]a_{i+q^j}-a_{i+q^{j+1}}}{\alpha_j^{(i+q^j)}}\cdot\frac{G_{i+q^j}(T)}{g_{i+q^j}}.$$

Now

$$\sum_{j=0}^{d(m)}\sum_{i=0}^{q^{j+1}-q^j-1}\frac{(-1)^{j+1}a_{i+q^{j+1}}G_{i+q^j}(T)}{\alpha_j^{(i+q^j)}g_{i+q^j}}=\sum_{j=0}^{d(m)}\sum_{i=0}^{q^j-q^{j-1}-1}\frac{(-1)^j a_{i+q^j}G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})}g_{i+q^{j-1}}},$$

where we have made use of the convention that $G_{i+q^{-1}}=0$, $a_{i+q^{d(m)+1}}=0$. Hence, every $f\in D^1$ can be expressed in the required basis.

On the other hand, suppose we are given an integer-valued polynomial written in this basis, called B_{ij} for short, over $\mathrm{GF}[q,x]$, in the form

$$f(T)=A_0+\sum_{i,j}B_{ij}a_{i+q^j}.$$

Retreating the steps above, we can write f in the form

$$f(T)=A_0+\sum_{i,j}\frac{A_{i+q^j}G_{i+q^j}(T)}{g_{i+q^j}}\in\mathrm{IVP},$$

where $(-1)^j\alpha_j^{(i+q^j)}A_{i+q^j}=[j]a_{i+q^j}-a_{i+q^{j+1}}$, and

$$Df(T)=\sum_{i=0}^{m-1}\left\{\sum_{j=0}^{d(m-i)}\frac{[j]a_{i+q^j}-a_{i+q^{j+1}}}{L_j}\right\}\frac{G_i(T)}{g_i}=\sum_{i=0}^{m-1}\frac{a_{i+1}G_i(T)}{g_i}\in\mathrm{IVP},$$

where we have made used of the convention that $a_{i+q^{d(m-i)+1}}=0$.

Remarks. As witnessed by Theorem 2, and the remarks after Corollary 2, no basis for D^r is of simple form, yet repeated use of the arguments as in Theorem 2 can clearly be applied to obtain bases for all D^r, $r\geq 1$. We are content here to derive one more basis, that of D^2.

Theorem 3. *The set*

$$\Big\{1, \Big(\frac{[j]G_{i+q^j}(T)}{\alpha_j^{(i+q^j)} g_{i+q^j}} + \frac{\delta(i, q^j - q^{j-1} - 1)G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})} g_{i+q^{j-1}}}\Big)\frac{[j]}{\alpha_j^{(i-1+q^j)}}$$
$$-\Big(\frac{[j-1]G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})} g_{i+q^{j-1}}} + \frac{\delta(i, q^{j-1} - q^{j-2} - 1)G_{i+q^{j-2}}(T)}{\alpha_{j-2}^{(i+q^{j-2})} g_{i+q^{j-2}}}\Big)\frac{\delta(i, q^j - q^{j-1} - 1)}{\alpha_{j-1}^{(i-1+q^{j-1})}}$$
$$\text{for } j = 0, 1, 2, \ldots;\ i = 0, 1, \ldots, q^{j+1} - q^j - 1\Big\},$$

where the α*'s and* δ*'s are as defined in Theorem* 2, *forms a basis for* D^2 *over* $\mathrm{GF}[q, x]$, *provided that those terms with* α*'s* $\equiv 0 \pmod p$ *in the denominators are interpreted as* 0.

Remark. In the proof that follows, we proceed as if all the α's $\not\equiv 0 \pmod p$; necessary adjustments for the other case are easily taken care of as described in the proof of Theorem 2.

Proof (of Theorem 3). Let

$$f(T) = \sum_{i=0}^{m} A_i G_i(T)/g_i \in \mathrm{IVP}.$$

From the proof of Theorem 2, we have

$$\begin{aligned} f \in D^1 \Leftrightarrow\ & (-1)^j \alpha_j^{(i+q^j)} A_{i+q^j} = [j]a_{i+q^j} - a_{i+q^{j+1}} \\ & (i = 0, 1, \ldots, m-1;\ j = 0, 1, \ldots, d(m-i)) \\ & \text{where all } a_{i+q^j} \in \mathrm{GF}[q, x],\ a_{i+q^{d(m-i)+1}} = 0, \text{ and } f \in \mathrm{IVP} \\ \Leftrightarrow\ & Df(T) = \sum_{i=0}^{m-1} \frac{a_{i+1}G_i(T)}{g_i} \in \mathrm{IVP} \text{ and } f \in \mathrm{IVP} \\ \Leftrightarrow\ & f(T) = A_0 + \sum_{j=0}^{d(m)} \sum_{i=0}^{q^{j+1}-q^j-1} (-1)^j \Big\{\frac{[j]G_{i+q^j}(T)}{\alpha_j^{(i+q^j)} g_{i+q^j}} \\ & \qquad + \frac{\delta(i, q^j - q^{j-1} - 1)G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})} g_{i+q^{j-1}}}\Big\} a_{i+q^j}. \end{aligned}$$

Repeated use of these facts implies that

$$\begin{aligned} f \in D^2 \Leftrightarrow\ & f \in D^1 \text{ and } Df \in D^1 \\ \Leftrightarrow\ & f \in D^1 \text{ and } (-1)^j \alpha_j^{(i+q^j)} a_{i+1+q^j} = [j]b_{i+q^j} - b_{i+q^{j+1}} \\ & (i = 0, 1, \ldots, m-2;\ j = 0, 1, \ldots, d(m-1-i)), \\ & \text{where all } b_{i+q^j} \in \mathrm{GF}[q, x],\ b_{i+q^{d(m-i)+1}} = 0 \end{aligned}$$

$$\Leftrightarrow f(T) = A_0 + \sum_{j=0}^{d(m)} \sum_{i=0}^{q^{j+1}-q^j-1} (-1)^j \left\{ \frac{[j]G_{i+q^j}(T)}{\alpha_j^{(i+q^j)} g_{i+q^j}} + \frac{\delta(i, q^j - q^{j-1} - 1)G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})} g_{i+q^{j-1}}} \right\} \left\{ \frac{[j]b_{i-1+q^j} - b_{i-1+q^{j+1}}}{(-1)^j \alpha_j^{(i-1+q^j)}} \right\}$$

$$= A_0 + \sum_{j=0}^{d(m)} \sum_{i=0}^{q^{j+1}-q^j-1} \frac{E_{ij}[j]b_{i-1+q^j}}{\alpha_j^{(i-1+q^j)}} - \sum_{j=0}^{d(m)} \sum_{i=0}^{q^j-q^{j-1}-1} \frac{E_{i,j-1}b_{i-1+q^j}}{\alpha_{j-1}^{(i-1+q^{j-1})}}$$

$$= A_0 + \sum_{j=0}^{d(m)} \sum_{i=0}^{q^{j+1}-q^j-1} \left\{ \frac{E_{ij}[j]}{\alpha_j^{(i-1+q^j)}} - \frac{E_{i,j-1}\delta(i, q^j - q^{j-1} - 1)}{\alpha_{j-1}^{(i-1+q^{j-1})}} \right\} b_{i-1+q^j}$$

where

$$E_{ij} = \frac{[j]G_{i+q^j}(T)}{\alpha_j^{(i+q^j)} g_{i+q^j}} + \frac{\delta(i, q^j - q^{j-1} - 1)G_{i+q^{j-1}}(T)}{\alpha_{j-1}^{(i+q^{j-1})} g_{i+q^{j-1}}},$$

$E_{ij} := 0$ if $j < 0$, and $b_{i+q^{d(m-i)+1}} = 0$. The theorem thus follows.

Since D^r has no bases of simple form, it may be of interest to obtain equivalent results involving divisibility by L_i in the spirit of Proposition 3. Let $f(T) = \sum_{i=0}^{m} A_i G_i(T)/g_i \in \mathrm{IVP}$. Then

$$Df(T) = \sum_{i=0}^{m-1} \left\{ \sum_{j=0}^{d(m-i)} \frac{(-1)^j \alpha_j^{(i+q^j)} A_{i+q^j}}{L_j} \right\} \frac{G_i(T)}{g_i}$$

and so

$$Df \in \mathrm{IVP} \Leftrightarrow A'(i) := \sum_{j=0}^{d(m-i)} \frac{(-1)^j \alpha_j^{(i+q^j)} A_{i+q^j}}{L_j} \in \mathrm{GF}[q, x] \qquad (i = 0, 1, \ldots, m-1).$$

Similarly, we have

$$D^2 f(T) = \sum_{i_2=0}^{m-2} \left\{ \sum_{j_2=0}^{d(m-1-i_2)} \frac{(-1)^{j_2} \alpha_{j_2}^{(i_2+q^{j_2})} A'(i_2 + q^{j_2})}{L_{j_2}} \right\} \frac{G_{i_2}(T)}{g_{i_2}},$$

and so for $i_2 = 0, 1, \ldots, m-2$, we have

$$D^2 f \in \mathrm{IVP} \Leftrightarrow A''(i_2) := \sum_{j_2=0}^{d(m-1-i_2)} \frac{(-1)^{j_2} \alpha_{j_2}^{(i_2+q^{j_2})} A'(i_2 + q^{j_2})}{L_{j_2}} \in \mathrm{GF}[q, x]$$

$$= \sum_{j_2=0}^{d(m-1-i_2)} \sum_{j_1=0}^{d(m-i_2-q^{j_2})} \frac{(-1)^{j_2+j_1}\alpha_{j_2}^{(i_2+q^{j_2})}\alpha_{j_1}^{(i_2+q^{j_2}+q^{j_1})}A_{i_2+q^{j_2}+q^{j_1}}}{L_{j_2}L_{j_1}} \in \mathrm{GF}[q,x].$$

Arguing as above, and noting that since $\mathrm{GF}[q,x]$ is of characteristic p, it follows that $D^p f = 0$ for all $f \in \mathrm{GF}(q,x)[T]$, we have in general

THEOREM 4. *Let $r \in \mathbb{N}$, $r < p$, and let $f(T) = \sum_{i=0}^{m} A_i G_i(T)/g_i \in \mathrm{IVP}$. Then*

$$D^r f \in \mathrm{IVP} \Leftrightarrow A^{(r)}(i_r) \in \mathrm{GF}[q,x],$$

where

$$\begin{aligned} A^{(r)}(i_r) = & \sum_{j_r=0}^{d(m-r+1-i_r)} \sum_{j_{r-1}=0}^{d(m-r+2-i_r-q^{j_r})} \cdots \\ & \cdots \sum_{j_2=0}^{d(m-1-i_r-q^{j_r}-\ldots-q^{j_3})} \sum_{j_1=0}^{d(m-i_r-q^{j_r}-\ldots-q^{j_2})} (-1)^{j_r+\ldots+j_1} \\ & \times \alpha_{j_r}^{(i_r+q^{j_r})}\alpha_{j_{r-1}}^{(i_r+q^{j_r}+q^{j_{r-1}})}\ldots\alpha_{1}^{(i_r+q^{j_r}+\ldots+q^{j_1})} \\ & \times \frac{A_{i_r+q^{j_r}+\ldots+q^{j_1}}}{L_{j_r}L_{j_{r-1}}\ldots L_{j_1}} \quad (i_r = 0,1,\ldots,m-r). \end{aligned}$$

Our last theorem confirms that the cases of differences and derivatives of infinite order are of special character.

THEOREM 5. (i) *For a positive integer r, we have $\Delta^r \subset D^r$, and the inclusion can be strict.*

(ii) *$\Delta^\infty = D^\infty$.*

Proof. To prove (i), it is enough to consider the case $r < p$. Let $f(T) = \sum_{i=0}^{m} A_i G_i(T)/g_i \in \Delta^r$. By Proposition 3, $L_{e(i)}^{*(r)} \mid A_i$ for all i. Now by part (c) of the Lemma, we get

$$\tag{1} \begin{gathered} \binom{i_r + q^{j_r} + \ldots + q^{j_1}}{i_r + q^{j_r} + \ldots + q^{j_2}} \equiv \alpha_{j_1}^{(i_r+q^{j_r}+\ldots+q^{j_1})} \pmod p, \\ \vdots \\ \binom{i_r + q^{j_r}}{i_r} \equiv \alpha_{j_r}^{(i_r+q^{j_r})} \pmod p. \end{gathered}$$

By (1) and the shape of $A^{(r)}(i_r)$ in Theorem 4, we see that

$$L_{e(K-J_1)}L_{e(J_1-J_2)}\ldots L_{e(J_{r-1}-J_r)}A^{(r)}(i_r), \quad \text{where}$$
$$K = i_r + q^{j_r} + \ldots + q^{j_1}, \quad J_1 = i_r + q^{j_r} + \ldots + q^{j_2}, \ldots, J_r = i_r,$$

belongs to $\mathrm{GF}[q,x]$, and so $D^r f \in \mathrm{IVP}$ for all r. Thus $f \in D^r$, yielding $\Delta^r \subset D^r$. That, generally, $\Delta^r \neq D^r$ follows from the remarks after Corollary 2.

To prove (ii), by Corollary 3 we have

$$f \in \Delta^\infty \Leftrightarrow L^{*(\infty)}_{e(i)} \mid A_i \text{ for all } i,$$

where we use the convention that $L^{*(\infty)}_{e(0)} = 1$. By the same arguments as above, we thus get $A^{(r)}(i_r) \in \mathrm{GF}[q,x]$ for each positive integer r. This implies that $\Delta^\infty \subset D^\infty$.

Finally, to show that $D^\infty \subset \Delta^\infty$, take any $f(T) = \sum_{i=0}^m A_i G_i(T)/g_i \in D^\infty$. Since $D^p f = 0$, we have

$$\Delta f(T) = \frac{f(T+M) - f(T)}{M} = \sum_{i=1}^{p-1} \frac{M^{i-1} D^i f(T)}{i!} \in \mathrm{IVP},$$

i.e.

$$f \in D^\infty \Rightarrow \Delta f \in \mathrm{IVP}, \text{ and so } f \in \Delta. \tag{2}$$

In general,

$$\begin{aligned} D^j(\Delta f(T)) = \Delta(D^j f(T)) &= \frac{D^j f(T+M) - D^j f(T)}{M} \\ &= \begin{cases} \displaystyle\sum_{i=1}^{p-1-j} \frac{M^{i-1} D^{i+j} f(T)}{i!} \in \mathrm{IVP} & \text{if } j \le p-1, \\ 0 & \text{if } j \ge p, \end{cases} \end{aligned}$$

and so

$$\begin{aligned} f \in D^\infty &\Rightarrow \Delta f \in D^j \text{ for each positive integer } j \\ &\Rightarrow \Delta f \in D^\infty \\ &\Rightarrow f \in \Delta^2 \quad \text{by (2).} \end{aligned} \tag{3}$$

Repeated applications of (2) and (3) yield that $f \in \Delta^\infty$, and so $D^\infty \subset \Delta^\infty$.

Theorem 5 and Corollary 3 give

COROLLARY 4. *The set* $\{1, L^{*(\infty)}_{e(i)} G_i(T)/g_i : i = 1, 2, \ldots\}$ *forms a basis for* D^∞ *over* $\mathrm{GF}[q,x]$.

References

[1] D. Brizolis and E. G. Straus, *A basis for the ring of doubly integer-valued polynomials*, J. Reine Angew. Math. 286/287 (1976), 187–195.

[2] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. 1 (1935), 137–168.

[3] —, *A set of polynomials*, ibid. 6 (1940), 486–504.

[4] L. Carlitz, *Finite sums and interpolation formulas over* $\mathrm{GF}[p^n, x]$, ibid. 15 (1948), 1001–1012.
[5] —, *A note on integral-valued polynomials*, Indag. Math. 21 (1959), 294–298.
[6] L. Comtet, *Advanced Combinatorics*, Reidel, Dordrecht, 1974.
[7] N. G. de Bruijn, *Some classes of integer-valued functions*, Indag. Math. 17 (1955), 363–367.
[8] R. R. Hall, *On pseudo-polynomials*, Mathematika 18 (1971), 71–77.
[9] V. Laohakosol and P. Ubolsri, *A short note on integral-valued polynomials*, Southeast Asian Bull. Math. 4 (1980), 43–47.
[10] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Math. 1600, Springer, Berlin, 1995.
[11] G. Pólya and G. Szegő, *Problems and Theorems in Analysis*, Vol. II, Springer, New York, 1976.
[12] E. G. Straus, *On the polynomials whose derivatives have integral values at the integers*, Proc. Amer. Math. Soc. 2 (1951), 24–27.
[13] C. G. Wagner, *Linear operators in local fields of prime characteristic*, J. Reine Angew. Math. 251 (1971), 153–160.
[14] —, *Interpolation series for continuous functions on* π*-adic completions of* $\mathrm{GF}(q, x)$, Acta Arith. 17 (1971), 389–406.
[15] —, *Interpolation series in local fields of prime characteristic*, Duke Math. J. 39 (1972), 203–210.
[16] —, *Linear pseudo-polynomials over* $\mathrm{GF}[q, x]$, Arch. Math. (Basel) 25 (1974), 385–390.
[17] —, *Polynomials over* $\mathrm{GF}(q, x)$ *with integral-valued differences*, ibid. 27 (1976), 495–501.

Department of Mathematics
Kasetsart University
Bangkok 10900, Thailand
E-mail: fscivil@nontri.ku.ac.th

Received on 30.9.1997
and in revised form on 24.4.1998 (3274)