JP Journal of Algebra, Number Theory and Applications
© 2017 Pushpa Publishing House, Allahabad, India
http://www.pphmj.com
http://dx.doi.org/10.17654/NT039061003
Volume 39, Number 6, 2017, Pages 1003-1022 **ISSN: 0972-5555**

A DESCRIPTION OF A DRINFELD MODULE WITH CLASS NUMBER $h = 1$ AND RANK 1

Victor Bautista-Ancona[1], Javier Diaz-Vargas[1], José Alejandro Lara Rodríguez[1] and Francisco X. Portillo-Bobadilla[2]

[1]Universidad Autónoma de Yucatán
México

[2]Universidad Autónoma de la Ciudad de México
México

Abstract

We work out in detail the Drinfeld module over the ring

$$A = \mathbb{F}_2[x, y]/(y^2 + y = x^3 + x + 1).$$

The example in question is one of the four examples that come from quadratic imaginary fields with class number $h = 1$ and rank one.

We develop specific formulas for the coefficients d_k and ℓ_k of the exponential and logarithmic functions and relate them with the product D_k of all monic elements of A of degree k. On the Carlitz module, D_k and d_k coincide, but this is not true for general Drinfeld modules. On this example, we obtain a formula relating both invariants. We prove also using elementary methods a theorem due to Thakur that relate two different combinatorial symbols important in the analysis of solitons.

Received: July 4, 2017; Revised: August 5, 2017; Accepted: August 22, 2017
2010 Mathematics Subject Classification: 11G09.
Keywords and phrases: Drinfeld module, exponential and logarithmic functions.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p and K be a function field over $\mathbb{F}_q$. After we choose ∞, a fixed infinite place of K, let A be the ring of regular functions outside of ∞ and let K_∞ be its completion. Now take $\mathbb{C}_\infty$ to be the completion of an algebraic closure of K_∞.

Let $\mathbb{C}_\infty\{\tau\}$ be the ring of *twisted polynomials*, i.e., the noncommutative ring of polynomials $\sum a_i \tau^i$ with coefficients in $\mathbb{C}_\infty$ such that $\tau z = z^q \tau$. A twisted polynomial $f = a_0 + a_1\tau + \cdots + a_d\tau^d \in \mathbb{C}_\infty\{\tau\}$ is identified with the $\mathbb{F}_q$-linear endomorphism of $\mathbb{C}_\infty$,

$$z \mapsto f(z) = a_0 z + a_1 z^q + \cdots + a_d z^{q^d}.$$

A Drinfeld A-module is an $\mathbb{F}_q$-algebra homomorphism $\rho : A \to \mathbb{C}_\infty\{\tau\}$ injective, for which $\rho(a) = a\tau^0 + \text{higher}$ order terms in τ. The action $a \cdot z = \rho(a)(z)$ of A in $\mathbb{C}_\infty$ makes $\mathbb{C}_\infty$ into an A-module, and hence the name "Drinfeld module".

For each Drinfeld module ρ we associate an exponential entire function e defined by a power series

$$e(z) = \sum_{i=0}^{\infty} \frac{z^{q^i}}{d_i} \text{ for all } z \in \mathbb{C}_\infty.$$

This exponential function satisfies the following fundamental functional equation:

$$e(az) = \rho_a(e(z)), \tag{1}$$

for $z \in \mathbb{C}_\infty$ and $a \in A$, where ρ_a stands for $\rho(a)$.

The Carlitz module, defined by Carlitz [1] in 1935, is given by the $\mathbb{F}_q$-algebra homomorphism $C : \mathbb{F}_q[t] \to \mathbb{C}_\infty\{\tau\}$ determined by $C_t = t + \tau^q$.

Equation (1) produces $e(tz) = te(z) + e(z)^q$. It follows that

$$\sum_{i=0}^{\infty} \frac{(t^{q^i} - t) z^{q^i}}{d_i} = \sum_{i=0}^{\infty} \frac{z^{q^{i+1}}}{d_i^q}.$$

By equating coefficients we get a unique solution $d_n = [n] d_{n-1}^q$, where $[n] = (t^{q^n} - t)$ and $d_0 = 1$. Therefore, $d_n = [n][n-1]^q \cdots [1]^{q^{n-1}}$ and it is easily seen that d_n is the product of all monic polynomials of degree n.

Since $e(z)$ is periodic, it cannot have a global inverse, but we may formally derive an inverse $\log(z)$ for $e(z)$ as a power series around the origin. By definition $e(\log(z)) = z$. Since $e(z)$ satisfies the functional equation $e(tz) = te(z) + e(z)^q$, it follows that $tz = \log(te(z)) + \log(e(z)^q)$. Replacing $\log(z)$ for z we obtain $t\log(z) = \log(tz) + \log(z^q)$. Let $\log(z) = \sum z^{q^i} / \ell_i$. Then

$$\sum_{i=0}^{\infty} \frac{(t - t^{q^i}) \cdot z^{q^i}}{\ell_i} = \sum_{i=0}^{\infty} \frac{z^{q^{i+1}}}{\ell_i}.$$

It follows that $\ell_{i+1} = -[i+1]\ell_i$. Therefore $\ell_i = (-1)^i [i][i-1] \cdots [1]$.

We follow the ideas developed in the Carlitz module case, but applied to the Drinfeld module over $A = \mathbb{F}_2[x, y]/(y^2 + y = x^3 + x + 1)$. We explore specific ways to understand the mentioned example, which is one of four examples provided from imaginary quadratic fields with class number $h = 1$ [4] and rank 1. The formulas obtained are compared with Theorem 4.15.4 of [5] and are related to solitons, as exposed in Chapter 8 of the same reference, and Theorem 3 of the article [6].

2. Action of the Drinfeld Module on the Variables x and y

In our example, we have $d_\infty = 1$, $v_\infty(x) = -2$, $v_\infty(y) = -3$, and using that $\deg(a) = -v_\infty(a)d_\infty, \ \forall a \in A,$ it follows that $\deg(x) = 2$ and $\deg(y) = 3.$

Based on it, the Drinfeld module ρ that we are considering has rank 1 and is determined by its values in x and y (actually, it is enough to know its value in one element $a \in A,$ see 2.5 in [5]). According to the aforementioned degrees and that the unique sign in our example is +1, we obtained that

$$\rho_x = x + x_1\tau + \tau^2,$$

$$\rho_y = y + y_1\tau + y_2\tau^2 + \tau^3$$

with $x_1, y_1, y_2 \in A.$ Now, using the commutative property of the Drinfeld module $\rho_x\rho_y = \rho_y\rho_x$ and equating on degree 1, we get

$$x_1(y^2 + y) = y_1(x^2 + x).$$

Next, using the equation on the curve $y^2 + y = x^3 + x + 1$ and dividing, we obtain

$$y_1 = x_1\left(x + 1 + \frac{1}{x^2 + x}\right).$$

This implies that $x^2 + x \mid x_1$ and $y^2 + y \mid y_1.$ Assuming that $x_1 = x^2 + x,$ it is also obtained that $y_1 = y^2 + y.$ Now, equating on degree 2, one has the equation

$$(x^4 + x)y_2 = -y_1x_1^2 + y_1^2x_1 + (y^4 + y). \tag{2}$$

But, we can use the identities

$$\begin{aligned} y^4 + y &= (y^2 + y)^2 + y^2 + y \\ &= (y^2 + y)(y^2 + y + 1) \\ &= (y^2 + y)(x^3 + x) \\ &= (y^2 + y)(x^2 + x)(x + 1) \end{aligned}$$

and

$$x^4 + x = (x^2 + x)(x^2 + x + 1).$$

So dividing the equation (2) by $x_1 = x^2 + x,$ and substituting the values x_1 and $y_1,$ we get

$$\begin{aligned} y_2(x^2 + x + 1) &= (y^2 + y)(x^2 + x + y^2 + y) + (y^2 + y)(x + 1) \\ &= (y^2 + y)(y^2 + y + x^2 + 1) \\ &= (y^2 + y)(x^3 + x^2 + x). \end{aligned}$$

Thus, clearing $x^2 + x + 1,$ we have $y_2 = x(y^2 + y),$ as it is known in the literature [3, Example 11.3].

3. Exponential and Logarithm Coefficients

We find recursive formulas for the coefficients of both the exponential $e(z)$ and the logarithmic $\log(z)$ functions associated to the Drinfeld module from Section 2.

Write

$$e(z) = \sum_{i=0}^{\infty} \frac{z^{2^i}}{d_i} = \sum_{i=0}^{\infty} a_i z^{2^i}$$

and

$$\log(z) = \sum_{i=0}^{\infty} \frac{z^{2^i}}{\ell_i} = \sum_{i=0}^{\infty} b_i z^{2^i},$$

where $a_i = d_i^{-1}$ and $b_i = \ell_i^{-1}.$ Using that

$$\begin{aligned} e(xz) &= \rho_x(e(z)) \\ &= xe(z) + [1]_x e^2(z) + e^4(z), \end{aligned}$$

where $[1]_x = x^2 + x.$ Then, expanding both sides of the equality:

$$e(xz) + xe(z) = [1]_x e^2(z) + e^4(z),$$

we have on the left side:

$$\begin{aligned} e(xz) + xe(z) &= \sum_{j=0}^{\infty} (x^{2^j} + x) a_j z^{2^j} \\ &= \sum_{j=0}^{\infty} [j]_x a_j z^{2^j} \\ &= [1]_x a_1 z^2 + \sum_{j=2}^{\infty} [j]_x a_j z^{2^j}, \end{aligned} \tag{3}$$

where $[j]_x := x^{2^j} + x.$ Now, expanding the right side, we get:

$$[1]_x e^2(z) + e^4(z) = [1]_x \sum_{i=0}^{\infty} a_i^2 z^{2^{i+1}} + \sum_{i=0}^{\infty} a_i^4 z^{2^{i+2}}.$$

By setting $j = i + 1$ in the first sum, and $j = i + 2$ in the second sum, we obtain:

$$\begin{aligned} [1]_x e^2(z) + e^4(z) &= [1]_x \sum_{j=1}^{\infty} a_{j-1}^2 z^{2^j} + \sum_{j=2}^{\infty} a_{j-2}^4 z^{2^j} \\ &= [1]_x a_0^2 z^2 + \sum_{j=2}^{\infty} ([1]_x a_{j-1}^2 + a_{j-2}^4) z^{2^j}. \end{aligned} \tag{4}$$

Comparing equations (3) and (4), recursive formulas are obtained

$$\begin{aligned} a_1 &= a_0^2, \\ a_j &= \frac{[1]_x a_{j-1}^2 + a_{j-2}^4}{[j]_x} \text{ for } j \geq 2. \end{aligned} \tag{5}$$

Subsequently, we assume that $a_0 = 1,$ i.e., the exponential is normalized. Notice that if we do not normalize the coefficients, the exponential function varies by a factor given by the initial term. If we denote $e(z, a_0)$ to this exponential function, it is easy to see that

$$e(z, a_0) = a_0 e(z), \tag{6}$$

where $e(z)$ is the normalized exponential.

Now, in terms of the d_j's (assuming also, the normalization of the exponential), the recursive formula is as follows:

$$d_1 = d_0^2 = 1,$$

$$d_j = \frac{[j]_x d_{j-1}^2 d_{j-2}^4}{[1]_x d_{j-2}^4 + d_{j-1}^2} \text{ for } j \geq 2. \tag{7}$$

Similarly, for the logarithm function, we have that

$$\begin{aligned} x\log(z) &= \log(\rho_x(z)) \\ &= \log(xz + [1]_x z^2 + z^4) \\ &= \log(xz) + \log([1]_x z^2) + \log(z^4), \end{aligned}$$

from which it follows that

$$x\log(z) + \log(xz) = \log([1]_x z^2) + \log(z^4).$$

So, we expanded the left side to

$$\begin{aligned} x\log(z) + \log(xz) &= \sum_{j=0}^{\infty} (x^{2^j} + x) b_j z^{2^j} \\ &= \sum_{j=1}^{\infty} [j]_x b_j z^{2^j}. \end{aligned} \tag{8}$$

Note that $[0]_x = 0.$ The right side must be

$$\log([1]_x z^2) + \log(z^4) = \sum_{i=0}^{\infty} [1]_x^{2^i} b_i z^{2^{i+1}} + \sum_{i=0}^{\infty} b_i z^{2^{i+2}}.$$

Again, by setting $j = i+1$ in the first sum, and $j = i+2$ in the second sum, we obtain

$$\log([1]_x z^2) + \log(z^4) = [1]_x b_1 z^2 + \sum_{j=2}^{\infty} ([1]_x^{2^{j-1}} b_{j-1} + b_{j-2}) z^{2^j}. \tag{9}$$

Comparing the terms in the equations (8) and (9), we obtain the recursive formulas:

$$b_1 = b_0,$$

$$b_j = \frac{[1]_x^{2^{j-1}} b_{j-1} + b_{j-2}}{[j]_x} \text{ for } j \geq 2. \tag{10}$$

Now again, if $\log(z, b_0)$ is the logarithmic function with initial term b_0, and $\log(z) = \log(z, 1)$ is the normalized logarithm, by the recursion formula, we deduce the relation:

$$\log(z, b_0) = b_0 \log(z). \tag{11}$$

In terms of values ℓ_i's, the recursions are as follows:

$$\ell_1 = \ell_0,$$

$$\ell_j = \frac{[j]_x \ell_{j-1} \ell_{j-2}}{[1]_x^{2^{j-1}} \ell_{j-2} + \ell_{j-1}} \text{ for } j \geq 2.$$

4. Formulæ for Computing ρ_a

The first formula is recursive and is in the spirit of Proposition 3.3.10 in [2].

Assume that $\rho_a = \sum_{k=0}^{d} \rho_{a,k}\tau^k$ with $d = \deg(a)$. We will use again commutativity $\rho_x\rho_a = \rho_a\rho_x$ and the explicit expression: $\rho_x = x + [1]_x\tau + \tau^2$. Then, multiplying

$$\rho_x\rho_a = (x + [1]_x\tau + \tau^2)\left(\sum_{k=0}^{d} \rho_{a,k}\tau^k\right)$$

$$= \sum_{k=0}^{d} (x\rho_{a,k}\tau^k + [1]_x\rho_{a,k}^2\tau^{k+1} + \rho_{a,k}^4\tau^{k+2})$$

and multiplying

$$\rho_a\rho_x = \left(\sum_{k=0}^{d} \rho_{a,k}\tau^k\right)(x + [1]_x\tau + \tau^2)$$

$$= \sum_{k=0}^{d} (x^{2^k}\rho_{a,k}\tau^k + [1]_x^{2^k}\rho_{a,k}\tau^{k+1} + \rho_{a,k}\tau^{k+2}).$$

By comparing terms a recursive formula is obtained

$$\rho_{a,0} = a \qquad \text{(first term in recursion)},$$

$$\rho_{a,1} = a^2 + a \qquad \text{(comparing degree } k = 1),$$

$$\rho_{a,k} = \frac{[1]_x^{2^{k-1}}\rho_{a,k-1} + \rho_{a,k-2}}{[k]_x} + \frac{[1]_x\rho_{a,k-1}^2 + \rho_{a,k-2}^4}{[k]_x}, \text{ for } k \geq 2.$$

Note the similarity to the recursive formulas for a_j's and b_j's in the previous section, equations (5) and (10). The same phenomenon occurs in the Carlitz module, but in such a case, there is only a single summand.

Another way to calculate ρ_a, is based on the use of the exponential and the logarithm functions and their formal development as power series. We know that

$$e(a\log(z)) = \rho_a(e(\log(z))) = \rho_a(z).$$

Using power series as in the previous section, we get to

$$\rho_a(z) = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} a_j b_{k-j}^{2^j} a^{2^j}\right) z^{2^k}$$

$$= \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} \frac{a^{2^j}}{d_j \ell_{k-j}^{2^j}}\right) z^{2^k}.$$

The combinatorial terms in the sum, are the ones that Thakur used to develop his alternative perspective on solitons [6].

We introduce the following notation used hereafter:

$$p_k(w) := \begin{Bmatrix} w \\ q^k \end{Bmatrix} := \sum_{j=0}^{k} \frac{w^{2^j}}{d_j \ell_{k-j}^{2^j}}.$$

Hence, since $\rho_a = \sum \rho_{a,k}\tau^k$ is a monic polynomial in τ of degree $\deg(a)$, we have that $p_k(a) = 0$ if $\deg(a) < k$; and $p_k(a) = 1$ if $\deg(a) = k$.

5. Comparing the Polynomials $p_k(w)$ and $e_k(w)$

Define the following sets:

$$A_{<k} := \{a \in A : \deg(a) < k\},$$

$$A_k := \{a \in A : \deg(a) = k\}$$

and the polynomial

$$e_k(w) = \prod_{a \in A_{<k}} (w + a).$$

Clearly, by the last paragraph in the previous Section 4, every $a \in A_{<k}$ is a root of $p_k(w)$. Thus,

$$R_k(w) := \frac{p_k(w)}{e_k(w)}$$

is a polynomial. In addition, as $p'_k(w) = a_k = \ell_k^{-1} \neq 0,$ $p_k(w)$ and $R_k(w)$ have no double roots.

In order to calculate the polynomial $R_k(w),$ suppose

$$p_k(w) = \sum_{i=0}^{k} A_{k,i} w^{2^i}$$

and

$$e_k(w) = \sum_{i=0}^{k-1} B_{k,i} w^{2^i}. \tag{12}$$

Then, we have the following result:

Theorem 5.1. $R_k(w) = \frac{1}{d_k} e_k(w) + C,$ *where* $C = \frac{1}{d_{k-1}} + \frac{B_{k,k-2}^2}{d_k}.$

Proof. Only for the purpose of this proof, suppose k is fixed and write $A_i = A_{k,i}$ and $B_i = B_{k,i}$. Now, directly dividing p_k by $e_k,$ using that e_k is monic, the first term of the quotient ratio is $A_k w^{2^{k-1}}$. Then, in the first line of the long division, we have:

$$A_k B_{k-2} w^{2^{k-1}+2^{k-2}} + A_k B_{k-3} w^{2^{k-1}+2^{k-3}} + \cdots +$$

$$A_k B_0 w^{2^{k-1}+1} + A_{k-1} w^{2^{k-1}} + \text{ lower terms.}$$

This implies that the next term of the quotient is $A_k B_{k-2} w^{2^{k-2}},$ and therefore, multiplying by the summands of $e_k,$ after cancellation of the term $A_k B_{k-2} w^{2^{k-1}+2^{k-2}},$ new summands will be incorporated into the residue in the positions corresponding to the powers:

$$w^{2^{k-1}},\ w^{2^{k-2}+2^{k-3}},\ \dots,\ w^{2^{k-2}+1}.$$

Hence, all the new terms fall into the "lower terms" of the long division with exception of the coefficient on $w^{2^{k-1}}$. This coefficient is $A_{k-1} + A_k B_{k-2}^2$.

When continuing the division and canceling the terms of the form $A_k B_j w^{2^{k-1}+2^j}$ for $j < k-2$, the terms equal or higher to $w^{2^{k-1}}$ are not affected. This ensures that the obtained quotient is:

$$A_k w^{2^{k-1}} + A_k B_{k-2} w^{2^{k-2}} + A_k B_{k-3} w^{2^{k-3}} + \cdots + A_k B_0 w + A_{k-1} + A_k B_{k-2}^2.$$

The result follows, using that $A_k = d_k^{-1}$ and $A_{k-1} = d_{k-1}^{-1}$. □

6. Coefficient Formulas for $e_k(w)$

For $k \geq 2$, set

$$t_k = \begin{cases} x^{\frac{k}{2}}, & \text{if } k \text{ is even,} \\ yx^{\frac{k-3}{2}}, & \text{if } k \text{ is odd.} \end{cases}$$

Now, it is clear that $\deg(t_k) = k$ and that the set $\{1, t_2, \dots, t_{k-1}\}$ is a basis of the vector space $A_{<k}$. Define $D_k := e_k(t_k) = \prod_{a \in A_k} a$. Thus, for $k \geq 3$,

$$\begin{aligned} e_k(w) &= \prod_{a \in A_{<k}} (w + a) = \prod_{a \in A_{<k-1}} (w + a) \prod_{a \in A_{k-1}} (w + a) \\ &= \prod_{a \in A_{<k-1}} (w + a) \prod_{a \in A_{<k-1}} (w + t_{k-1} + a) \\ &= e_{k-1}(w) e_{k-1}(w + t_{k-1}) = e_{k-1}^2(w) + D_{k-1} \cdot e_{k-1}(w). \end{aligned} \tag{13}$$

Expanding the right side of the equation (13), we find recursive formulas for the coefficients $B_{k,i}$ in (12):

$$e_{k-1}^2(w) + D_{k-1} \cdot e_{k-1}(w) = \left(\sum_{i=0}^{k-2} B_{k-1,i} w^{2^i}\right)^2 + D_{k-1}\left(\sum_{i=0}^{k-2} B_{k-1,i} w^{2^i}\right)$$

$$= \sum_{i=1}^{k-1} B_{k-1,i-1}^2 w^{2^i} + \sum_{i=0}^{k-2} D_{k-1} B_{k-1,i} w^{2^i}.$$

Indeed, we have

$$B_{k,0} = D_{k-1} B_{k-1,0} = D_{k-1} D_{k-2} \cdots D_2,$$

$$B_{k,i} = D_{k-1} B_{k-1,i} + B_{k-1,i-1}^2,$$

$$B_{k,k-1} = B_{k-1,k-2} = \cdots = B_{2,1} = 1.$$

Before developing explicit formulas for the coefficients $B_{k,i}$, we introduce the following symbols:

$$[1]_w = w^2 + w,$$

$$[k]_w = w^{2^k} + w.$$

It is not difficult to prove that these symbols satisfy the following:

Lemma 6.1. *Properties of the symbol* $[k]_w$.

(1) $[k]_w^{2^j} = [k]_{w^{2^j}}$,

(2) $[1]_{[k]_w} = [k]_{[1]_w}$,

(3) $[k]_{w_1+w_2} = [k]_{w_1} + [k]_{w_2}$,

(4) $[k+1]_w = [k]_w^2 + [1]_w$,

(5) $[k]_w = \sum_{i=0}^{k-1} [1]_w^{2^i}$.

Notice that $e_k(w)$ is a polynomial on $[1]_w$ of degree 2^{k-2}. Set

$$e_k(w) = \sum_{i=0}^{k-2} T_{k,i} [1]_w^{2^i}.$$

Next, we will find specific formulas for the coefficients $T_{k,i}$'s. First, define the following functions:

$$S_{n,r}(x_1, x_2, \ldots, x_n) = \sum_{n \geq i_1 > i_2 > \cdots > i_r \geq 1} \prod_{j=1}^{r} x_{i_j}^{2^{n-j+1-i_j}}.$$

We have the following lemma:

Lemma 6.2. *Properties of the sums* $S_{n,r}(x_1, x_2, \ldots, x_n)$.

(1) $S_{n,0}(x_1, \ldots, x_n) = 1$,

(2) $S_{n,1}(x_1, \ldots, x_n) = x_n + x_{n-1}^2 + \cdots + x_1^{2^{n-1}}$,

(3) $S_{n+1,r}(x_1, \ldots, x_{n+1}) = S_{n,r}^2(x_1, \ldots, x_n) + x_{n+1} S_{n,r-1}(x_1, \ldots, x_n)$.

Proof. The first two assertions are immediate.

For the third, note that:

$$S_{n,r}^2(x_1, \ldots, x_n) = \left(\sum_{n \geq i_1 > i_2 > \cdots > i_r \geq 1} \prod_{j=1}^{r} x_{i_j}^{2^{n-j+1-i_j}} \right)^2$$

$$= \sum_{n \geq i_1 > i_2 > \cdots > i_r \geq 1} \prod_{j=1}^{r} x_{i_j}^{2^{n+1-j+1-i_j}}. \qquad (14)$$

On the other hand,

$$x_{n+1}S_{n,r-1}(x_1, \ldots, x_n) = x_{n+1} \sum_{n \geq i_1 > i_2 > \cdots > i_{r-1} \geq 1} \prod_{j=1}^{r-1} x_{i_j}^{2^{n-j+1-i_j}}$$

$$= \sum_{n \geq i_1 > i_2 > \cdots > i_{r-1} \geq 1} x_{n+1} \prod_{j=1}^{r-1} x_{i_j}^{2^{n-j+1-i_j}}. \tag{15}$$

Now, making $i_1 = n+1$ and $i_{j+1} = i_j$ (moving the variable j to $j+1$), we obtain that (15) becomes

$$\sum_{n+1 = i_1 > i_2 > \cdots > i_r \geq 1} \prod_{j=1}^{r} x_{i_j}^{2^{n+1-j+1-i_j}}. \tag{16}$$

Notice that the variable x_{i_j} with exponent $n - j + 1 - i_j$ in (15) coincide with the variable $x_{i_{j+1}}$ with exponent $n + 1 - j + 1 - i_{j+1}$ in (16).

Now, clearly the sum of (14) and (16) proves the lemma. □

Proposition 6.3. *For*

$$e_k(w) = \sum_{i=0}^{k-2} T_{k,i}[1]_w^{2^i},$$

the following holds

$$T_{k,i} = S_{k-2,k-2-i}(D_2, D_3, \ldots, D_{k-1}),$$

where

$$D_i = e_i(t_i).$$

Proof. Using the identity

$$e_{k+1}(w) = e_k^2(w) + D_k e_k(w), \text{ for } k \geq 2,$$

we obtain the following recursive equations:

$$T_{k+1,0} = D_k T_{k,0},$$

$$T_{k+1,i} = T_{k,i-1}^2 + D_k T_{k,i},$$

$$T_{k+1,k-1} = 1.$$

Then, from induction suppose that the proposition is valid for $T_{k,i}$, using the recursive form, we get

$$T_{k+1,i} = T_{k,i-1}^2 + D_k T_{k,i}$$

$$= S_{k-2,k-2-(i-1)}^2(D_2, D_3, ..., D_{k-1}) + D_k S_{k-2,k-2-i}(D_2, D_3, ..., D_{k-1})$$

$$= S_{k-2,k-1-i}^2(D_2, D_3, ..., D_{k-1}) + D_k S_{k-2,k-1-i-1}(D_2, D_3, ..., D_{k-1})$$

$$= S_{k-1,k-1-i}(D_2, D_3, ..., D_k).$$

The last equality follows from Lemma 6.2. Now, the result follows from verifying that the coefficients $T_{k,i}$ coincide with $S_{k-2,k-2-i}(D_2, D_3, ..., D_{k-1})$ for some first small values of k. □

For simplicity, set $S_{k-2,k-2-i} \coloneqq S_{k-2,k-2-i}(D_2, D_3, ..., D_{k-1})$.

Corollary 6.4. *The coefficients of the polynomial*

$$e_k(w) = \sum_{i=0}^{k-1} B_{k,i} w^{2^i}$$

are given by the formulas

$$B_{k,k-1} = T_{k,k-2} = S_{k-2,0} = 1,$$

$$B_{k,i} = T_{k,i} + T_{k,i-1} = S_{k-2,k-2-i} + S_{k-2,k-1-i}, \textit{ for } 1 \le i \le k-2,$$

$$B_{k,0} = T_{k,0} = S_{k-2,k-2} = D_{k-1} D_{k-2} \cdots D_2.$$

Proof. Note that

$$e_k(w) = \sum_{i=0}^{k-2} T_{k,i}[1]_w^{2^i}$$

$$= \sum_{i=0}^{k-2} T_{k,i}(w + w^2)^{2^i}$$

$$= T_{k,k-2}w^{2^{k-1}} + \sum_{i=1}^{k-2}(T_{k,i} + T_{k,i-1})w^{2^i} + T_{k,0}w. \qquad \square$$

7. Relationship Among the Values d_k, ℓ_k and D_k

Basically, these relationships are corollary of Theorem 5.1 and the explicit expression of the coefficients $B_{k,i}$ developed in the previous section.

If we evaluate the polynomial equality

$$p_k(w) = \frac{e_k^2(w)}{d_k} + Ce_k(w) \tag{17}$$

in $w = t_k$, we get that

$$1 = \frac{D_k^2}{d_k} + CD_k.$$

Solving for C, we obtain

$$C = \frac{1}{D_k} + \frac{D_k}{d_k} = \frac{d_k + D_k^2}{D_k d_k}. \tag{18}$$

Now, using the definition of C in (5.1), we also have that

$$C = \frac{1}{d_{k-1}} + \frac{1 + D_{k-1}^2 + D_{k-2}^4 + \cdots + D_2^{2^{k-2}}}{d_k},$$

since

$$B_{k,k-2}^2 = (1 + D_{k-1} + D_{k-2}^2 + \cdots + D_2^{2^{k-3}})^2,$$

from Corollary 6.4 and part (2) of Lemma 6.2.

Multiplying by $D_k d_k$, we obtain

$$CD_k d_k = \frac{D_k d_k}{d_{k-1}} + D_k(1 + D_{k-1}^2 + D_{k-2}^4 + \cdots + D_2^{2^{k-2}})$$

and using (18), we have

$$d_k + D_k^2 = \frac{D_k d_k}{d_{k-1}} + D_k(1 + D_{k-1}^2 + D_{k-2}^4 + \cdots + D_2^{2^{k-2}}).$$

Therefore

$$d_k\left(1 + \frac{D_k}{d_{k-1}}\right) = D_k(1 + D_k + D_{k-1}^2 + \cdots + D_2^{2^{k-2}}),$$

and hence

$$d_k = \frac{D_k d_{k-1}}{d_{k-1} + D_k}(1 + D_k + D_{k-1}^2 + \cdots + D_2^{2^{k-2}})$$

$$= \frac{D_k d_{k-1}}{d_{k-1} + D_k} \cdot B_{k+1,k-1}. \tag{19}$$

Now, using the recursive formula (7) is easy to see that

$$d_2 = [1]_x$$

and also

$$D_2 = e_2(t_2) = [1]_{t_2} = [1]_x,$$

equation (19) gives a recursive procedure to calculate d_k, in terms of values D_i's with $2 \le i \le k$.

Now, equating the coefficients of the linear terms of the polynomials in (17), we obtain that

$$\frac{1}{\ell_k} = CD_{k-1}D_{k-2} \cdots D_2$$

and using (18), we conclude that

$$\ell_k = \frac{D_k d_k}{(d_k + D_k^2)(D_{k-1}D_{k-2} \cdots D_2)}.$$

We summarize the above discussion in the main result of the article.

Theorem 7.1. *Recursive formulas to compute* ℓ_k *and* d_k *values in terms of* D_k*' s,*

(1) $d_2 = D_2,$

(2) $d_k = \frac{D_k d_{k-1}}{d_{k-1} + D_k}(1 + D_k + D_{k-1}^2 + \cdots + D_2^{2^{k-2}}),$

(3) $\ell_k = \frac{D_k d_k}{(d_k + D_k^2)(D_{k-1}D_{k-2} \cdots D_2)}.$

Acknowledgements

Francisco Portillo thanks Conacyt for financial support for a sabbatical stay at Universidad Autónoma de Yucatán under the project grant #261761.

The authors also thank the anonymous referees for their valuable suggestions which led to the improvement of the manuscript.

References

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

[2] D. Goss, Basic Structures of Function Field Arithmetic, 2nd ed., Springer-Verlag, 1998.

[3] D. R. Hayes, Explicit Class Field Theory in Global Function Fields, Studies in Algebra and Number Theory, G. C. Rota, ed., Academic Press, San Diego, 1979, pp. 173-217.

[4] R. E. MacRae, On unique factorization in certain rings of algebraic functions, J. Algebra 17 (1971), 77-91.

[5] D. S. Thakur, Function Field Arithmetic, World Scientific Publishing Co. Pvt. Ltd., 2004.

[6] D. S. Thakur, An alternate approach to solitons for $F_q[t]$, Journal of Number Theory 76 (1999), 301-319.