ACTA ARITHMETICA
101.1 (2002)

Transcendence, automata theory and gamma functions for polynomial rings

by

ZHI-YING WEN (Beijing) and JIA-YAN YAO (Wuhan)

1. Introduction. Let $p \geq 2$ be a prime and $q = p^s$ with $s \in \mathbb{N}$ $(s \geq 1)$. Denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_q[T]$ the integral domain of polynomials with coefficients in $\mathbb{F}_q$. The fraction field of $\mathbb{F}_q[T]$ is denoted by $\mathbb{F}_q(T)$. It was shown in [11] that a value of the Carlitz–Goss gamma function $\overline{\Pi}_T$ is transcendental over $\mathbb{F}_q(T)$ if and only if the argument is not an element of $\mathbb{N} = \{0, 1, 2, \ldots\}$. Using the same idea and that of [3], we shall show that a value of the T-adic Carlitz–Goss gamma function Π_T is transcendental over $\mathbb{F}_q(T)$ if and only if the q-adic coefficients of the argument are not ultimately constant.

For the convenience of the reader, we shall sometimes give more details than needed for this purpose.

2. Carlitz gamma function. The factorial function Π for the ring $\mathbb{F}_q[T]$ was first introduced by L. Carlitz [4].

For any $j \in \mathbb{N}$, let D_j be the product of all monic polynomials of degree j, i.e.,

$$D_j = \prod_{\substack{P \text{ monic in } \mathbb{F}_q[T] \\ \deg P = j}} P.$$

In particular we have $D_0 = 1$. Now define the *factorial function* Π as follows.

For each $n \in \mathbb{N}$ with standard q-adic expansion $n = \sum_{j=0}^{k} n_j q^j$ $(0 \leq n_j \leq q-1)$, put $\Pi(n) := \prod_{j=0}^{k} D_j^{n_j}$. The gamma function Γ is defined by $\Gamma(n+1) := \Pi(n)$.

Let P be a monic prime polynomial. Denote by v_P the P-adic valuation, i.e., for every $Q \in \mathbb{F}_q[T]$, $v_P(Q)$ is the greatest integer k such that P^k divides

2000 *Mathematics Subject Classification*: Primary 11T55, 11B85; Secondary 68Q70.
Key words and phrases: Carlitz–Goss gamma functions, transcendence, automatic sequences.

Q in $\mathbb{F}_q[T]$. With these definitions and notations, we have

$$\Pi(n) = \prod_{P\,\text{monic prime}} P^{n_P} \tag{1}$$

where for each monic prime polynomial P, $n_P := v_P(\Pi(n)) = \sum_{l=1}^{\infty} \lfloor n/N(P)^l \rfloor$, $N(P)$ is the cardinality of the residue class field $\mathbb{F}_q[T]/P\mathbb{F}_q[T]$, i.e., $N(P) = q^{\deg P}$ and for any real number x, $\lfloor x \rfloor$ means the integral part of x.

Relation (1) noticed by W. Sinnott explains partially why Π is called the factorial function (we refer to [12] and the references there for several other reasons why Π and Γ are good analogues of the classical factorial and gamma functions). In fact, this prime polynomial factorization is an exact analogue of the classical prime number factorization formula

$$n! = \prod_{r\,\text{prime}} r^{n_r} \tag{2}$$

where for each prime number r, $n_r = \sum_{l=1}^{\infty} \lfloor n/N(r)^l \rfloor$ and $N(r)$ is the cardinality of the residue class field $\mathbb{Z}/r\mathbb{Z}$, i.e., $N(r) = r$.

The analogy between (1) and (2) reveals a surprising similarity between the two integral domains $\mathbb{F}_q[T]$ and $\mathbb{Z}$. Note in particular that the multiplicative group $\mathbb{F}_q[T]^\times$ of $\mathbb{F}_q[T]$ is $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$ and $\mathbb{Z}^\times = \{1, -1\}$, thus monic polynomials correspond to positive integers and monic prime polynomials correspond to prime numbers (see [12] for more discussion).

3. Some properties of the integral domain $\mathbb{F}_q[T]$. We give two well known results useful for our later study.

LEMMA 1. *For each $j \in \mathbb{N}$ $(j \geq 1)$, we have*

$$[j] := T^{q^j} - T = \prod_{\substack{P\,\text{monic prime in}\,\mathbb{F}_q[T] \\ \deg P | j}} P. \tag{3}$$

Proof. Let Ω_p be an algebraic closure of $\mathbb{F}_p$. The set of all roots of $[j]$ in Ω_p forms a subfield of Ω_p isomorphic to the finite field $\mathbb{F}_{q^j}$. Let $P \in \mathbb{F}_q[T]$ be a monic prime polynomial of degree l and $\alpha \in \Omega_p$ be a root of P. The field $\mathbb{F}_q(\alpha)$ is a $\mathbb{F}_q$-vector space of dimension l, thus isomorphic to $\mathbb{F}_{q^l}$. But $\mathbb{F}_{q^l}$ is a subfield of $\mathbb{F}_{q^j}$ if and only if $l \,|\, j$. Moreover P divides $[j]$ in $\mathbb{F}_q[T]$ if and only if $[j](\alpha) = 0$, which is equivalent to saying that $\mathbb{F}_{q^l}$ is a subfield of $\mathbb{F}_{q^j}$. So P divides $[j]$ in $\mathbb{F}_q[T]$ if and only if l divides j. But $\mathbb{F}_q[T]$ is factorial and every root in Ω_p of $[j]$ is simple, so $[j]$ is the product of all monic prime polynomials in $\mathbb{F}_q[T]$ whose degree divides j. ■

LEMMA 2. *For each $j \in \mathbb{N}$ $(j \geq 1)$, we have*

$$D_j = \prod_{l=0}^{j-1} [j-l]^{q^l} = \prod_{l=0}^{j-1} (T^{q^j} - T^{q^l}).$$

Proof. For any fixed $j \in \mathbb{N}$ $(j \geq 1)$, put $B_j = \prod_{l=0}^{j-1} [j-l]^{q^l}$. Since D_j and B_j are monic and the integral domain $\mathbb{F}_q[T]$ is factorial, we need only show that for any monic prime polynomial $P \in \mathbb{F}_q[T]$ of degree d, we have $v_P(D_j) = v_P(B_j)$.

Clearly for $j < d$, $v_P(D_j) = v_P(B_j) = 0$. We can thus assume $j \geq d$.

By Lemma 1, for any $l \in \mathbb{N}$ $(l \geq 1)$, the monic polynomial $[l]$ is the product of all monic prime polynomials in $\mathbb{F}_q[T]$ whose degrees divide l. So $v_P([l])$ equals 0 or 1 and $v_P([l]) = 1$ if and only if d divides l. Consequently,

$$v_P(B_j) = \sum_{l=0}^{j-1} q^l v_P([j-l]) = \sum_{k=1}^{\lfloor j/d \rfloor} q^{j-kd}.$$

For each $m \in \mathbb{N}$, define $S_m = \{Q \in \mathbb{F}_q[T] \mid Q \text{ monic and } \deg Q = m\}$. Clearly S_m has q^m elements. But for any $m \in \mathbb{N}$ $(m \geq d)$, obviously $Q \in S_m$ is a multiple of P if and only if $Q \in PS_{m-d}$. Thus $v_P(D_m) = q^{m-d} + v_P(D_{m-d})$ for any $m \in \mathbb{N}$ satisfying $m \geq d$. By recurrence, we obtain $v_P(D_j) = \sum_{k=1}^{\lfloor j/d \rfloor} q^{j-kd} = v_P(B_j)$. ∎

Now we give a proof of the prime polynomial factorization formula (1).

Let P be a monic prime polynomial of degree d. For each $n \in \mathbb{N}$ with standard q-adic expansion $n = \sum_{j=0}^{k} n_j q^j$ $(0 \leq n_j \leq q-1)$, by virtue of Lemma 2, we have

$$n_P := v_P(\Pi(n)) = \sum_{j=1}^{k} n_j v_P(D_j) = \sum_{j=1}^{k} n_j \sum_{l=1}^{\lfloor j/d \rfloor} q^{j-ld}.$$

By interchanging the last two summations, we obtain immediately

$$n_P = \sum_{l=1}^{\lfloor k/d \rfloor} \sum_{j=ld}^{k} n_j q^{j-ld} = \sum_{l=1}^{\lfloor k/d \rfloor} \lfloor n/q^{dl} \rfloor = \sum_{l=1}^{\infty} \lfloor n/N(P)^l \rfloor.$$

4. Carlitz–Goss gamma functions. We give a quick introduction to Carlitz–Goss gamma functions $\overline{\Pi}_T$ and Π_T (in fact the "true" Carlitz–Goss gamma functions $\overline{\Gamma}_T$ and Γ_T are defined by $\overline{\Gamma}_T(n) = \overline{\Pi}_T(n-1)$ and $\Gamma_T(n) = \Pi_T(n-1)$ for any p-adic integer $n \in \mathbb{Z}_p$). They were invented by D. Goss to interpolate the factorial function Π (see [8], [10], [12], [9] and their references for more discussion).

We begin with the ∞-adic interpolation $\overline{\Pi}_T$. For any $Q \in \mathbb{F}_q[T]$, its ∞-adic valuation $v_\infty(Q)$ is just $-\deg Q$. Extend v_∞ over $\mathbb{F}_q(T)$ and denote by $\mathbb{F}_q((T^{-1}))$ the topological completion of $\mathbb{F}_q(T)$ about v_∞. Then for any $f \in \mathbb{F}_q((T^{-1}))$, we can write $f = \sum_{l=k}^{\infty} a(l)T^{-l}$ with $v_\infty(f) = k \in \mathbb{Z}$, where for any $l \in \mathbb{Z}$ ($l \geq k$), we have $a(l) \in \mathbb{F}_q$ and $a(k) \neq 0$.

For each $j \in \mathbb{N}$, define $\overline{D}_j := D_j/T^{\deg D_j}$. By Lemma 2, we have $\deg D_j = jq^j$ and $v_\infty(\overline{D}_j - 1) = (q-1)q^{j-1}$ if $j \geq 1$. Then $\overline{D}_j$ tends to 1 in $\mathbb{F}_q((T^{-1}))$ as $j \to \infty$. So for $n \in \mathbb{Z}_p$ with $n = \sum_{j=0}^{\infty} n_j q^j$ $(0 \leq n_j \leq q-1)$, the infinite product

$$\overline{\Pi}_T(n) := \prod_{j=0}^{\infty} \overline{D}_j^{n_j} := \lim_{k\to\infty} \prod_{j=0}^{k} \overline{D}_j^{n_j}$$

converges and defines an element of $\mathbb{F}_q((T^{-1}))$.

Using rather different methods, many authors have studied the transcendence of certain particular values of $\overline{\Pi}_T$ (see e.g. [12], [13], [14] and [3]). J.-P. Allouche was the first to introduce automata theory in the study of Carlitz–Goss gamma functions (cf. [2] and [3]). By following his idea but improving his method, M. Mendès France and J.-Y. Yao showed the theorem below (cf. [11]):

Theorem 1. *For each $n \in \mathbb{Z}_p$, the formal Laurent series $\overline{\Pi}_T(n)$ is transcendental over the field $\mathbb{F}_q(T)$ if and only if $n \notin \mathbb{N}$.*

In duality with the ∞-adic valuation v_∞, we have the T-adic valuation v_T and the corresponding T-adic interpolation Π_T.

Denote by $\mathbb{F}_q((T))$ the T-adic completion of $\mathbb{F}_q(T)$. Then every formal power series $f \in \mathbb{F}_q((T))$ takes the form $f = \sum_{l=k}^{\infty} a(l)T^{l}$ with $v_T(f) = k \in \mathbb{Z}$, where for any $l \in \mathbb{Z}$ ($l \geq k$), we have $a(l) \in \mathbb{F}_q$ and $a(k) \neq 0$.

For any $j \in \mathbb{N}$, denote by $D_{j,T}$ the product of all monic polynomials in $\mathbb{F}_q[T]$ of degree j which are prime to T. Trivially $D_{0,T} = D_0 = 1$. Now fix $j \in \mathbb{N}$ such that $j \geq 1$. Clearly in $\mathbb{F}_q[T]$, a monic polynomial of degree j is divisible by T if and only if it is a product of T with a monic polynomial of degree $j-1$. But there are exactly q^{j-1} monic polynomials of degree $j-1$. So $D_{j,T} = D_j/T^{q^{j-1}} D_{j-1}$.

In [8], D. Goss showed that $-D_{j,T}$ tends T-adically to 1 as $j \to \infty$. Below we reproduce his proof which is quite simple and instructive.

Fix $j \in \mathbb{N}$ $(j > 1)$. If $Q \in \mathbb{F}_q[T]$ is a monic polynomial of degree j, we can decompose Q into $Q = T^j + B$ with $\deg B < \deg T^j = j$. Clearly Q and T are coprime if and only if B and T are coprime. Denote by $(\mathbb{F}_q[T]/T^j\mathbb{F}_q[T])^\times$ the multiplicative group of $\mathbb{F}_q[T]/T^j\mathbb{F}_q[T]$. For any $g \in (\mathbb{F}_q[T]/T^j\mathbb{F}_q[T])^\times$, $g = g^{-1}$ if and only if $g = \pm 1 \pmod{T^j}$, hence we have

$$\prod_{g \in (\mathbb{F}_q[T]/T^j\mathbb{F}_q[T])^\times} g = -1.$$

Note that for any $B \in \mathbb{F}_q[T]$ with $\deg B < j$, the residue class $B \pmod{T^j}$

contains only one monic polynomial of degree j. Then we have

$$D_{j,T}=\prod_{\substack{\gcd(Q,T)=1\\ \deg Q=j}} Q \equiv \prod_{\substack{\gcd(B,T)=1\\ \deg B<j}} B \pmod{T^j} \equiv -1 \pmod{T^j},$$

which implies that $-D_{j,T}$ tends T-adically to 1 as $j\to\infty$. Thus for any p-adic integer $n\in\mathbb{Z}_p$ with $n=\sum_{j=0}^{\infty} n_j q^j$ $(0\le n_j\le q-1)$, the infinite product

$$\Pi_T(n):=\prod_{j=0}^{\infty}(-D_{j,T})^{n_j}$$

converges and defines an element of $\mathbb{F}_q((T))$.

Analogous to Theorem 1, we have a similar result about Π_T.

THEOREM 2. *Let $n=\sum_{j=0}^{\infty} n_j q^j$ $(0\le n_j\le q-1)$ be a p-adic integer. Then $\Pi_T(n)$ is algebraic over $\mathbb{F}_q(T)$ if and only if the sequence $(n_j)_{j\ge0}$ is ultimately constant.*

5. Proof of the sufficiency of Theorem 2. Let $n\in\mathbb{Z}_p$ be a p-adic integer with $n=\sum_{j=0}^{\infty} n_j q^j$ $(0\le n_j\le q-1)$ such that the sequence $(n_j)_{j\ge0}$ is ultimately constant. We shall show that $\Pi_T(n)$ is algebraic over $\mathbb{F}_q(T)$. Note that if we change a finite number of terms of $(n_j)_{j\ge0}$, we do not change the nature of $\Pi_T(n)$. So we can assume $n_j=d$ for all $j\in\mathbb{N}$. Then we have

$$\Pi_T(n)=\prod_{j=0}^{\infty}(-D_{j,T})^{d}.$$

Put $H=\prod_{j=0}^{\infty}(-D_{j,T})$. Then $\Pi_T(n)=H^d$ and we need only show that the infinite product H is algebraic over $\mathbb{F}_q(T)$.

For any $k\in\mathbb{N}$ $(k\ge1)$, put $H_k:=\prod_{j=0}^{k}(-D_{j,T})$. Then H_k tends T-adically to H as $k\to\infty$. But $D_{j,T}=D_j/T^{q^{j-1}}D_{j-1}$ for any $j\in\mathbb{N}$ $(j\ge1)$, hence

$$H_k=(-1)^{k+1}D_kT^{-(q^k-1)/(q-1)}.$$

By Lemma 2, we have $D_k=\prod_{j=0}^{k-1}[k-j]^{q^j}$. Thus $D_k=D_{k-1}^q[k]$. Note also that in the field $\mathbb{F}_{q^d}$, we have $(-1)^q=-1$. Then

$$\frac{H_k}{H_{k-1}^q}=-\frac{[k]}{T}=\frac{T-T^{q^k}}{T},$$

which implies $H=H^q$, i.e., H is algebraic over the field $\mathbb{F}_q(T)$. ∎

6. Elements of automata theory. In this section, we recall some basic definitions, notations and results in automata theory. The reader can also consult [1] and [6] for a more general discussion on this subject.

Let E be a finite nonempty set. We call it an *alphabet* and denote by $\mathrm{Card}(E)$ or $|E|$ the number of elements in E. Every element in E is called a *letter*. Fix $\emptyset$ an element not in E and call it an *empty letter* over E.

Take $n \in \mathbb{N}$. If $n = 0$, define $E^0 := \{\emptyset\}$. For $n \geq 1$, denote by E^n the set of all finite sequences of length n with elements in E. Let $E^* := \bigcup_{n=0}^{\infty} E^n$. Every element w of E^* is called a *word* over E and its length is denoted by $|w|$. More precisely, for $w \in E^n$, we define $|w| := n$. In particular $|\emptyset| = 0$.

Let $w, v \in E^*$ be two words over E. The concatenation of w and v (denoted by $w * v$ or more simply by wv) is again a word over E defined as follows:

$$(w * v)(n) = \begin{cases} w(n) & \text{if } 0 \leq n < |w|, \\ v(n - |w|) & \text{if } |w| \leq n < |w| + |v|. \end{cases}$$

In particular, for any $w \in E^*$, we have $w\emptyset = \emptyset w = w$. Obviously $(E^*, *)$ is a monoid with $\emptyset$ as the identity element.

Now we give a definition of a finite automaton (see for example [7]):

A *finite automaton* $\mathcal{A} = (S, i, \Sigma, t)$ (called a Σ-*automaton*) consists of

- an alphabet S of states; one state i is distinguished and called the *initial state*;
- a map $t : S \times \Sigma \to S$, called a *transition function*, where Σ is an alphabet containing at least two elements.

For any $A \in S$, put $t(A, \emptyset) = A$. Extend t over $S \times \Sigma^*$ (denoted again by t) such that for all $A \in S$ and $l, m \in \Sigma^*$, we have

$$t(A, lm) = t(t(A, l), m).$$

Fix $r \in \mathbb{N}$ $(r \geq 2)$ and set $\Sigma_r := \{0, 1, \ldots, r-1\}$. We call $u = (u(n))_{n\geq 0}$ an r-*automatic sequence* if there exist a finite automaton $\mathcal{A} = (S, i, \Sigma_r, t)$ and a map o defined on S with values in another alphabet Y such that $u(0) = o(i)$ and for any $n \in \mathbb{N}$ $(n \geq 1)$ with standard r-adic expansion $n = \sum_{j=0}^{\lfloor \log n/\log r \rfloor} n_j r^j$, we have

$$u(n) = o(t(i, n_k \ldots n_0)).$$

In this case we also say that u is *generated* by $(\mathcal{A}, o)$. In particular, if o is the identity map of S, we say simply that u is generated by the finite automaton $\mathcal{A}$.

Below we give a simple characterization of automatic sequences (see e.g. [1]).

THEOREM 3. *A sequence $u = (u(n))_{n\geq 0}$ is r-automatic if and only if its r-kernel*

$$\mathcal{N}_r(u) := \{(u(r^b n + a))_{n\geq 0} \mid b \geq 0,\ 0 \leq a < r^b\}$$

is a finite set.

This result can be found in a slightly different form in [7] (Prop. 3.3, p. 107). It was also quoted by G. Christol in [5], p. 141.

Remark 1. All ultimately periodic sequences are r-automatic.

Remark 2. From Theorem 3, we can deduce easily that a sequence is r-automatic if and only if it is r^k-automatic for all $k \in \mathbb{N}$ ($k \geq 1$).

Remark 3. Let $u = (u(n))_{n\geq 0}$ and $v = (v(n))_{n\geq 0}$ be two r-automatic sequences with terms in a semigroup. The r-kernel of the sequence $w = (u(n)v(n))_{n\geq 0}$ is finite, so w is also r-automatic.

The theorem below reveals a surprising relationship between automatic sequences and algebraic formal power series over a finite field and forms the cornerstone of modern automata theory (see [5], [6] and [1] for more details).

Theorem 4. *Let $\mathbb{F}_r$ be the finite field with r elements and $u=(u(n))_{n\geq 0}$ be a sequence with terms in $\mathbb{F}_r$. Then u is r-automatic if and only if the formal power series $\sum_{n=0}^{\infty} u(n)T^n$ is algebraic over the field $\mathbb{F}_r(T)$.*

This result, due to G. Christol, T. Kamae, M. Mendès France and G. Rauzy, appeared in [6]. A previous version of this theorem can be found in [5] which was published one year before the joint paper [6].

Remark 4. Let $f = \sum_{n=k}^{\infty} u(n)T^n$ with $k \in \mathbb{Z}$ be a formal power series in $\mathbb{F}_r((T))$. The derivative of f with respect to T is defined as $f' := \sum_{n=k}^{\infty} nu(n)T^{n-1}$. Let t be the characteristic of the finite field $\mathbb{F}_r$. The sequence $(n \pmod t)_{n\geq 0}$ is ultimately periodic, so by Remark 1, it is r-automatic. So if f is algebraic over $\mathbb{F}_r(T)$, from Theorem 4 and Remark 3, we know that the derivative f' of f is also algebraic over $\mathbb{F}_r(T)$. Actually, this result holds for any field in place of $\mathbb{F}_r$.

7. An application of Theorem 4.

We begin with a simple lemma.

Lemma 3. *Let $a, b, c, r \in \mathbb{N}$ be such that $a, b, c \geq 1$ and $r \geq 2$. Then $r^c - 1$ divides $r^a(r^b - 2) + 1$ if and only if $c \mid \gcd(a, b)$.*

Proof. This was shown in [11]. For completeness, we reproduce the proof below.

If $c \mid \gcd(a, b)$, then $r^c - 1$ divides $r^{a+b} - 1$, $r^a - 1$. So $r^c - 1 \mid r^a(r^b - 2) + 1$, for

$$r^a(r^b - 2) + 1 = (r^{a+b} - 1) - 2(r^a - 1).$$

The sufficiency is thus established.

Now we show the necessity. Suppose $r^c - 1 \mid r^a(r^b - 2) + 1$. Let a_1 and b_1 be two natural numbers such that $0 \leq a_1, b_1 < c$, $a_1 \equiv a + b \pmod c$ and $b_1 \equiv a \pmod c$. Write $a + b = mc + a_1$ and $a = nc + b_1$. For any $k \in \mathbb{N}$

$(k \geq 1)$, $r^c - 1 \mid r^{kc} - 1$ and

$$r^{a_1} - 2r^{b_1} + 1 = (r^a(r^b - 2) + 1) - r^{a_1}(r^{mc} - 1) + 2r^{b_1}(r^{nc} - 1),$$

therefore $r^c - 1 \mid r^{a_1} - 2r^{b_1} + 1$. But $|r^{a_1} - 2r^{b_1} + 1| < r^c - 1$ since $0 \leq a_1, b_1 < c$ and $r \geq 2$, hence $r^{a_1} + 1 = 2r^{b_1}$, which implies $a_1 = b_1 = 0$, i.e., $c \mid \gcd(a, b)$. ∎

The following theorem is the most important step towards Theorem 2. The idea of its proof is quite similar to that of Theorem 1 in [11].

Theorem 5. *Let $\mathbb{F}_r$ be the finite field with r elements and $u = (u(n))_{n \geq 1}$ be a sequence in $\mathbb{F}_r$. Then the formal power series in $\mathbb{F}_r((T))$ defined by*

$$f := \sum_{n=1}^{\infty} \frac{u(n)T^{r^n}}{T^{r^n} - T}$$

is algebraic over $\mathbb{F}_r(T)$ if and only if the sequence u is ultimately zero.

Proof. The sufficiency is quite evident. Now we show the necessity. Assume that f is algebraic over $\mathbb{F}_r(T)$ but u is not ultimately zero. Clearly

$$f = -\sum_{n=1}^{\infty} \frac{u(n)T^{r^n-1}}{1 - T^{r^n-1}} = -\sum_{n=1}^{\infty} u(n)T^{r^n-1} \sum_{l=0}^{\infty} T^{l(r^n-1)}$$
$$= -\sum_{n=1}^{\infty}\sum_{l=1}^{\infty} u(n)T^{l(r^n-1)} = -\sum_{m=0}^{\infty} c(m)T^m,$$

where $c(0) = 0$ and for any $m \in \mathbb{N}$ $(m \geq 1)$, $c(m)$ is defined by

$$c(m) := \sum_{\substack{n,l \geq 1 \\ m = l(r^n - 1)}} u(n) = \sum_{\substack{n \geq 1 \\ r^n - 1 \mid m}} u(n).$$

By Theorem 4, to obtain a contradiction, it suffices to show that $(c(m))_{m \geq 0}$ is not r-automatic. Put $C = \{m \in \mathbb{N} \mid u(m) \neq 0\}$. By our hypothesis on u, the set C is infinite. For any $t \in \mathbb{N}$ $(t \geq 1)$, set $c_t := (c(r^t m + 1))_{m \geq 0}$. Obviously $c_t \in \mathcal{N}_r(c)$. Let $a, b \in C$ $(a > b)$. We shall show $c_a \neq c_b$, which implies directly that $\mathcal{N}_r(c)$ is infinite for C is. Thus by Theorem 3, the sequence $(c(m))_{m \geq 0}$ is not r-automatic.

Put $V = \{m \in \mathbb{N} \mid u(m) \neq 0, m \mid a \text{ and } m \nmid b\}$. The set V is not empty as $a \in V$. Let h be the least element of V. If there exists $m \in \mathbb{N}$ $(1 \leq m < h)$ such that $m \mid h$ and $m \nmid b$, we necessarily have $u(m) = 0$. Hence by Lemma 3,

$$c_a(r^h - 2) - c_b(r^h - 2) = \sum_{r^m - 1 \mid r^a(r^h - 2) + 1} u(m) - \sum_{r^n - 1 \mid r^b(r^h - 2) + 1} u(n)$$
$$= \sum_{m \mid \gcd(a,h)} u(m) - \sum_{n \mid \gcd(b,h)} u(n)$$

$$= \sum_{m|h} u(m) - \sum_{n|\gcd(b,h)} u(n) \quad \text{(for } h \text{ divides } a)$$

$$= \sum_{\substack{m|h \\ m\nmid\gcd(b,h)}} u(m) = \sum_{m|h,\, m\nmid b} u(m) = u(h) \neq 0.$$

This ends the proof of our theorem. ∎

8. Proof of the necessity of Theorem 2. Let $n \in \mathbb{Z}_p$ be a p-adic integer such that $n = \sum_{j=0}^{\infty} n_j q^j$ $(0 \le n_j \le q-1)$. Suppose that the sequence $(n_j)_{j\ge 0}$ is not ultimately constant. We show that $\Pi_T(n)$ is transcendental over $\mathbb{F}_q(T)$. We distinguish two cases.

Case I: *The sequence* $(n_j \pmod p)_{j\ge 0}$ *is not ultimately constant.* Taking the logarithmic derivative of $\Pi_T(n)$ with respect to T, we obtain

$$\frac{(\Pi_T(n))'}{\Pi_T(n)} = \sum_{j=0}^{\infty} n_j \frac{D'_{j,T}}{D_{j,T}} = \sum_{j=1}^{\infty} n_j \left(\frac{D'_j}{D_j} - \frac{D'_{j-1}}{D_{j-1}} - \frac{q^{j-1}}{T}\right),$$

where the prime denotes derivation with respect to T.

Since the integers in the preceding formula should be taken modulo p, we obtain

$$\frac{(\Pi_T(n))'}{\Pi_T(n)} + n_1\left(\frac{1}{T} - \frac{D'_1}{D_1}\right) = \sum_{j=2}^{\infty} n_j \left(\frac{D'_j}{D_j} - \frac{D'_{j-1}}{D_{j-1}}\right).$$

Recall that for any $j \in \mathbb{N}$ $(j \ge 1)$, we have $D_j = \prod_{l=0}^{j-1}(T^{q^j} - T^{q^l})$. Thus

$$\frac{D'_j}{D_j} = \sum_{l=0}^{j-1} \frac{(T^{q^j} - T^{q^l})'}{T^{q^j} - T^{q^l}} = -\frac{1}{T^{q^j} - T}.$$

From the two formulas above we deduce immediately

$$\frac{(\Pi_T(n))'}{\Pi_T(n)} + n_1\left(\frac{1}{T} + \frac{1}{T^q - T}\right) = -\sum_{j=2}^{\infty} n_j \left(\frac{1}{T^{q^j} - T} - \frac{1}{T^{q^{j-1}} - T}\right),$$

which implies

$$T\frac{(\Pi_T(n))'}{\Pi_T(n)} = -\frac{n_1 T^q}{T^q - T} - \sum_{j=2}^{\infty} n_j \left(\frac{T^{q^j}}{T^{q^j} - T} - \frac{T^{q^{j-1}}}{T^{q^{j-1}} - T}\right)$$

$$= \sum_{j=1}^{\infty} (n_{j+1} - n_j) \frac{T^{q^j}}{T^{q^j} - T}.$$

But $((n_{j+1} - n_j) \pmod p)_{j\ge 1}$ is not ultimately zero for $(n_j \pmod p)_{j\ge 0}$ is not ultimately constant. By Theorem 5, the formal power series $(\Pi_T(n))'/\Pi_T(n)$ is transcendental over $\mathbb{F}_q(T)$. Then by Remark 4, this is also true for $\Pi_T(n)$.

Case II: *The sequence* $(n_j \pmod p)_{j\ge 0}$ *is ultimately constant.* Since $(n_j)_{j\ge0}$ is bounded and not ultimately constant, we can find $k \in \mathbb{N}$ $(1 \le k < s = \log q/\log p)$ such that $(n_j \pmod{p^k})_{j\ge0}$ is ultimately constant but $(n_j \pmod{p^{k+1}})_{j\ge0}$ is not. Then there exist $a, d \in \mathbb{N}$ $(0 \le a < p^k)$ such that $p^k \mid n_j - a$ for any $j \ge d$. For every $j \in \mathbb{N}$, put $m_j = 0$ if $j < d$ and $m_j = (n_j - a)/p^k$ if $j \ge d$. Then $(m_j \pmod p)_{j\ge0}$ is not ultimately constant for $(n_j \pmod{p^{k+1}})_{j\ge0}$ is not. Using the same argument as in Case I, we know that the infinite product $\prod_{j=0}^{\infty}(-D_{j,T})^{m_j}$ is transcendental over the field $\mathbb{F}_q(T)$. Furthermore we have

$$\Pi_T(n) = \Pi_T\Big(\frac{aq^d}{1-q}\Big)\Big(\prod_{j=0}^{d-1}(-D_{j,T})^{n_j}\Big)\Big(\prod_{j=0}^{\infty}(-D_{j,T})^{m_j}\Big)^{p^k}$$

and by the sufficiency of Theorem 2, the formal power series $\Pi_T\big(\frac{aq^d}{1-q}\big)$ is algebraic over $\mathbb{F}_q(T)$. So the formal power series $\Pi_T(n)$ is transcendental over $\mathbb{F}_q(T)$. ∎

9. Some corollaries. As a matter of fact, we have just proved the result below.

Theorem 6. *Let k be a positive integer and let $(n_j)_{j\ge0}$ be a sequence of rational integers such that $(n_j \pmod{p^k})_{j\ge0}$ is not ultimately constant. Then the formal power series $\prod_{j=0}^{\infty}(-D_{j,T})^{n_j}$ is transcendental over the field $\mathbb{F}_q(T)$.*

As a corollary, we immediately obtain the following theorem.

Theorem 7. *Let $\lambda_1, \ldots, \lambda_k$ be rational integers and $n^{(i)} = \sum_{j=0}^{\infty} n_j^{(i)} q^j$ be p-adic integers with $0 \le n_j^{(i)} < q$ $(1 \le i \le k)$. Then $\prod_{i=1}^{k}(\Pi_T(n^{(i)}))^{\lambda_i}$ is transcendental over the field $\mathbb{F}_q(T)$ if and only if $(\sum_{i=1}^{k} \lambda_i n_j^{(i)})_{j\ge0}$ is not ultimately constant.*

10. Further studies. Until now we have only studied the simplest case. In this section, we discuss the general situation and put forward a conjecture.

We begin with the definition of Π_P where $P \in \mathbb{F}_q[T]$ is a monic prime polynomial of degree d. Let $\mathbb{F}_q(T)_P$ be the P-adic completion of $\mathbb{F}_q(T)$. For any $j \in \mathbb{N}$, denote by $D_{j,P}$ the product of all monic polynomials in $\mathbb{F}_q[T]$ of degree j which are prime to P. Then $D_{j,P} = D_j$ for $0 \le j < d$ and $D_{j,P} = D_j/P^{q^{j-d}}D_{j-d}$ for $j \ge d$. According to D. Goss (cf. [8]), $-D_{j,P}$ tends P-adically to 1 as $j \to \infty$. Then for each $n \in \mathbb{Z}_p$ with $n = \sum_{j=0}^{\infty} n_j q^j$ $(0 \le n_j \le q-1)$, the infinite product

$$\varPi_P(n) := \prod_{j=0}^{\infty}(-D_{j,P})^{n_j}$$

converges and defines a formal power series in $\mathbb{F}_q(T)_P$.

Inspired by Theorem 2, we conjecture the following result.

Conjecture. *Let $n = \sum_{j=0}^{\infty} n_j q^j$ $(0 \le n_j \le q-1)$ be a p-adic integer and let $P \in \mathbb{F}_q[T]$ be a monic prime polynomial of degree d. Then the formal power series $\varPi_P(n)$ is algebraic over the field $\mathbb{F}_q(T)$ if and only if the sequence $(n_j)_{j\ge 0}$ is ultimately periodic of period d, i.e., there exists $a \in \mathbb{N}$ such that $n_{j+d} = n_j$ for any $j \ge a$.*

The sufficiency part of our Conjecture is quite evident and can be shown analogously to Theorem 2 (see also [12]). In fact, we can assume $n_j = 0$ $(0 \le j < d)$ and $n_{k+d} = n_k$ $(k \ge d)$ with $d := \deg P$. Then

$$\varPi_P(n) = \prod_{j=d}^{2d-1}\Big(\prod_{l=0}^{\infty}(-D_{ld+j,P})\Big)^{n_j}.$$

For any $j \in \mathbb{N}$, put $H_j = \prod_{l=0}^{\infty}(-D_{ld+j,P})$. Thus $\varPi_P(n) = \prod_{j=d}^{2d-1} H_j^{n_j}$ and we need only show that for each $j \in \mathbb{N}$ $(d \le j < 2d)$, the infinite product H_j is algebraic over $\mathbb{F}_q(T)$.

Let $\alpha \in \varOmega_p$ be a root of P. By Lemma 1, α is an element of $\mathbb{F}_{q^d}$ and $\alpha = \alpha^{q^d}$. Put $X = T - \alpha$. The X-adic completion $\mathbb{F}_{q^d}((X))$ of $\mathbb{F}_{q^d}(T)$ is a finite separable extension of $\mathbb{F}_q(T)_P$. So by a field homomorphism, we can identify $\mathbb{F}_q(T)_P$ to a subfield of $\mathbb{F}_{q^d}((X))$ such that $v_X(f) = v_P(f)$ for all $f \in \mathbb{F}_q(T)_P$.

For $m \in \mathbb{N}$ $(m \ge 1)$, define $H_j(m) := \prod_{l=0}^{m}(-D_{ld+j,P})$. As $m \to \infty$, $H_j(m)$ tends P-adically to H_j. Hence $H_j(m)$ also tends X-adically to H_j. However for every $l \in \mathbb{N}$, we have $D_{ld+j,P} = D_{ld+j}/P^{q^{(l-1)d+j}} D_{(l-1)d+j}$. Then

$$H_j(m) = (-1)^{m+1}\left(\frac{D_{md+j}}{D_{j-d}}\right)P^{-(q^j(q^{-d}-q^{md}))/(1-q^d)}.$$

By Lemma 2, we obtain $D_{md+j} = \prod_{l=0}^{md+j-1}[md+j-l]^{q^l}$. Therefore

$$D_{md+j} = D_{(m-1)d+j}^{q^d}\prod_{l=0}^{d-1}[md+j-l]^{q^l}.$$

But in $\mathbb{F}_{q^d}$, we have $(-1)^q = -1$. Then after a simple calculation, we obtain

$$\frac{H_j(m)}{(H_j(m-1))^{q^d}} = -P^{-q^{j-d}}D_{j-d}^{q^d-1}\prod_{l=0}^{d-1}[j+md-l]^{q^l}.$$

Note that for every $l \in \mathbb{N}$ $(0 \le l < d)$, we also have

$$[j + md - l] = T^{q^{j+md-l}} - T = X^{q^{j+md-l}} - T + \alpha^{q^{j-l}}.$$

Hence as $m \to \infty$, we obtain

$$H_j = -H_j^{q^d} P^{-q^{j-d}} D_{j-d}^{q^d-1} \prod_{l=0}^{d-1} (-T + \alpha^{q^{j-l}})^{q^l},$$

which implies that the infinite product H_j is algebraic over $\mathbb{F}_q(T)$. ∎

The necessity part of the preceding conjecture seems more difficult. For the moment, we can only show the weaker result below.

THEOREM 8. *Let $n = \sum_{j=0}^{\infty} n_j q^j$ $(0 \le n_j \le q-1)$ be a p-adic integer and $P \in \mathbb{F}_q[T]$ be a monic prime polynomial of degree d such that $\Pi_P(n)$ is algebraic over $\mathbb{F}_q(T)$. Assume there exists $a \in \mathbb{N}$ such that for all $j \in \mathbb{N}$ $(j \ge a)$ and all $k \in \mathbb{N}$ $(1 \le k < d)$, $n_{jd+k} = n_k$. Then the sequence $(n_j)_{j\ge 0}$ is ultimately periodic of period d.*

COROLLARY. *When* $\deg P = 1$, *our Conjecture holds.*

The proof of Theorem 8, which is quite similar to that of Theorem 2, will be left as a good exercise to the reader.

Acknowledgments. We thank Jean-Paul Allouche and D. Thakur for some interesting discussions. We also thank National Natural Science Foundation of China and Morningside Center of Mathematics (CAS) for their financial support.

References

[1] J.-P. Allouche, *Automates finis en théorie des nombres*, Exposition. Math. 5 (1987), 239–266.

[2] —, *Sur la transcendance de la série formelle Π*, Sém. Théor. Nombres Bordeaux 2 (1990), 103–117.

[3] —, *Transcendence of the Carlitz–Goss gamma function at rational arguments*, J. Number Theory 60 (1996), 318–328.

[4] L. Carlitz, *An analogue of the von Staudt–Clausen theorem*, Duke Math. J. 3 (1937), 503–517.

[5] G. Christol, *Ensembles presques périodiques k-reconnaissables*, Theoret. Comput. Sci. 9 (1979), 141–145.

[6] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France 108 (1980), 401–419.

[7] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, 1974.

[8] D. Goss, *Modular forms for $\mathbb{F}_r[T]$*, J. Reine Angew. Math. 317 (1980), 16–39.

[9] —, *Basic Structures of Function Field Arithmetic*, Springer, New York, 1997.

[10] D. Goss, D. Hayes and M. Rosen (eds.), *The Arithmetic of Function Fields*, de Gruyter, Berlin, 1992.

[11] M. Mendès France and J.-Y. Yao, *Transcendence and the Carlitz–Goss gamma function*, J. Number Theory 63 (1997), 396–402.
[12] D. Thakur, *On Gamma functions for function fields*, in [10], 75–86.
[13] A. Thiery, *Indépendance algébrique des périodes et quasi-périodes d'un module de Drinfeld*, in [10], 265–284.
[14] J. Yu, *Transcendence in finite characteristic*, in [10], 253–264.

Department of Mathematics
Tsinghua University
Beijing 100084
People's Republic of China
E-mail: wenzy@tsinghua.edu.cn

Department of Mathematics
Nonlinear Science Center
Wuhan University
Wuhan 430072
People's Republic of China
E-mail: yaojiaya@public.wh.hb.cn

Received on 29.6.2000
and in revised form on 27.12.2000 (3843)