Christol's theorem and its analogue for generalized power series, part 1

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://math.ucsd.edu/~kedlaya/slides/

Challenges in Combinatorics on Words
Fields Institute, Toronto, April 26, 2013

This part based on: G. Christol, "Ensembles presque périodiques k-reconaissables", *Theoretical Computer Science* **9** (1979), 141–145; G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, "Suites algébriques, automates et substitutions", *Bull. Soc. Math. France* **108** (1980), 401–419; Chapter 12 of J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge Univ. Press, 2003.

Supported by NSF (grant DMS-1101343), UCSD (Warschawski chair).

Contents

Formal power series

Let K be any field. The ring of *formal power series* over K, denoted $K[\![t]\!]$, consists of formal infinite sums $\sum_{n=0}^{\infty} f_n t^n$ added term-by-term:

$$\sum_{n=0}^{\infty} f_n t^n + \sum_{n=0}^{\infty} g_n t^n = \sum_{n=0}^{\infty} (f_n + g_n) t^n$$

and multiplied by formal series multiplication (convolution):

$$\sum_{n=0}^{\infty} f_n t^n \times \sum_{n=0}^{\infty} g_n t^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} f_i g_{n-i} \right) t^n.$$

Formal Laurent series

A *formal Laurent series* over K is a formal doubly infinite sum $\sum_{n\in\mathbb{Z}} f_n t^n$ with $f_n \in K$ such that only finitely many of the f_n for $n < 0$ are nonzero. These again form a ring:

$$\sum_{n\in\mathbb{Z}} f_n t^n + \sum_{n\in\mathbb{Z}} g_n t^n = \sum_{n\in\mathbb{Z}} (f_n + g_n) t^n$$

$$\sum_{n\in\mathbb{Z}} f_n t^n \times \sum_{n\in\mathbb{Z}} g_n t^n = \sum_{n\in\mathbb{Z}} \left(\sum_{i+j=n} f_i g_j \right) t^n.$$

In fact these form a *field*, denoted $K((t))$. It is the fraction field of $K[\![t]\!]$.

Polynomials and power series

There is an obvious inclusion of the polynomial ring $K[t]$ into the formal power series ring $K\llbracket t \rrbracket$. Since $K((t))$ is a field, this extends to an inclusion of the rational function field $K(t)$ into the formal Laurent series field $K((t))$.

Proposition (easy)

The image of $K(t)$ in $K((t))$ consists of those formal Laurent series $\sum_{n\in\mathbb{Z}} f_n t^n$ for which the sequence $f_0, f_1, \dots$ satisfies a linear recurrence relation. That is, for some nonnegative integer m there exist $c_0, \dots, c_m \in K$ not all zero such that

$$c_0 f_n + \cdots + c_m f_{n+m} = 0 \qquad (n = 0, 1, \dots).$$

Algebraic dependence

Let $K \subseteq L$ be an inclusion of fields. An element $x \in L$ is *algebraic* over K (or *integral* over K) if there exists a monic polynomial $P[z] \in K[z]$ such that $P(x) = 0$. For example, $\sqrt{-1} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$.

Proposition

The set of $x \in L$ which are algebraic over K is a subfield of L.

Proof.

$x \in L$ is algebraic over K if and only if all powers of x lie in a finite-dimensional K-subspace of L. (We'll see the proof later.) □

Algebraic dependence for formal Laurent series

Let us specialize to the inclusion $K(t) \subset K((t))$.

Question

Can one give an explicit description of those elements of $K((t))$ which are algebraic over $K(t)$, analogous to the description of $K(t)$ in terms of coefficients?

Amazingly, when K is a finite field this question has an affirmative answer in terms of combinatorics on words!

Algebraic dependence for formal Laurent series

Let us specialize to the inclusion $K(t) \subset K((t))$.

Question

Can one give an explicit description of those elements of $K((t))$ which are algebraic over $K(t)$, analogous to the description of $K(t)$ in terms of coefficients?

Amazingly, when K is a finite field this question has an affirmative answer in terms of combinatorics on words!

Contents

Regular languages

Fix a finite set Σ as the *alphabet*. Let Σ^* denote the set of finite words on Σ. A *language* on Σ is a subset L of Σ^*. We write xy for the concatenation of the words x and y.

A *deterministic finite automaton* Δ on Σ consists of a finite *state set* S, an *initial state* $s_0 \in S$, and a *transition function* $\delta : S \times \Sigma \to S$. The automaton induces a function $g_\Delta : \Sigma^* \to S$ by

$$g_\Delta(\emptyset) = s_0, \qquad g_\Delta(x\sigma) = \delta(g_\Delta(x), \sigma).$$

Any language of the form $g_\Delta^{-1}(S_1)$ for some $S_1 \subseteq S$ is *accepted* by Δ.

Any language accepted by some automaton is said to be *regular*. It is equivalent to ask that the language be accepted by some regular expression or by some nondeterministic finite automaton. In particular, reversing all strings in a regular language yields a regular language.

Regular languages

Fix a finite set Σ as the *alphabet*. Let Σ^* denote the set of finite words on Σ. A *language* on Σ is a subset L of Σ^*. We write xy for the concatenation of the words x and y.

A *deterministic finite automaton* Δ on Σ consists of a finite *state set* S, an *initial state* $s_0 \in S$, and a *transition function* $\delta : S \times \Sigma \to S$. The automaton induces a function $g_\Delta : \Sigma^* \to S$ by

$$g_\Delta(\emptyset) = s_0, \qquad g_\Delta(x\sigma) = \delta(g_\Delta(x), \sigma).$$

Any language of the form $g_\Delta^{-1}(S_1)$ for some $S_1 \subseteq S$ is *accepted* by Δ.

Any language accepted by some automaton is said to be *regular*. It is equivalent to ask that the language be accepted by some regular expression or by some nondeterministic finite automaton. In particular, reversing all strings in a regular language yields a regular language.

Regular languages

Fix a finite set Σ as the *alphabet*. Let Σ^* denote the set of finite words on Σ. A *language* on Σ is a subset L of Σ^*. We write xy for the concatenation of the words x and y.

A *deterministic finite automaton* Δ on Σ consists of a finite *state set* S, an *initial state* $s_0 \in S$, and a *transition function* $\delta : S \times \Sigma \to S$. The automaton induces a function $g_\Delta : \Sigma^* \to S$ by

$$g_\Delta(\emptyset) = s_0, \qquad g_\Delta(x\sigma) = \delta(g_\Delta(x), \sigma).$$

Any language of the form $g_\Delta^{-1}(S_1)$ for some $S_1 \subseteq S$ is *accepted* by Δ.

Any language accepted by some automaton is said to be *regular*. It is equivalent to ask that the language be accepted by some regular expression or by some nondeterministic finite automaton. In particular, reversing all strings in a regular language yields a regular language.

Regular languages

Fix a finite set Σ as the *alphabet*. Let Σ^* denote the set of finite words on Σ. A *language* on Σ is a subset L of Σ^*. We write xy for the concatenation of the words x and y.

A *deterministic finite automaton* Δ on Σ consists of a finite *state set* S, an *initial state* $s_0 \in S$, and a *transition function* $\delta : S \times \Sigma \to S$. The automaton induces a function $g_\Delta : \Sigma^* \to S$ by

$$g_\Delta(\emptyset) = s_0, \qquad g_\Delta(x\sigma) = \delta(g_\Delta(x), \sigma).$$

Any language of the form $g_\Delta^{-1}(S_1)$ for some $S_1 \subseteq S$ is *accepted* by Δ.

Any language accepted by some automaton is said to be *regular*. It is equivalent to ask that the language be accepted by some regular expression or by some nondeterministic finite automaton. In particular, reversing all strings in a regular language yields a regular language.

More on regular languages

Let L be a language on Σ. Define an equivalence relation on Σ^* by declaring that $x \sim_L y$ if and only if for all $z \in \Sigma^*$, $xz \in L$ if and only if $yz \in L$.

Theorem (Myhill-Nerode)

The language L is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_L$.

Sketch of proof.

If L is accepted by a finite automaton, then any two words leading to the same state are equivalent. Conversely, if there are finitely many equivalence classes, these correspond to the states of a minimal finite automaton which accepts L. □

More on regular languages

Let L be a language on Σ. Define an equivalence relation on Σ^* by declaring that $x \sim_L y$ if and only if for all $z \in \Sigma^*$, $xz \in L$ if and only if $yz \in L$.

Theorem (Myhill-Nerode)

The language L is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_L$.

Sketch of proof.

If L is accepted by a finite automaton, then any two words leading to the same state are equivalent. Conversely, if there are finitely many equivalence classes, these correspond to the states of a minimal finite automaton which accepts L. □

More on regular languages

Let L be a language on Σ. Define an equivalence relation on Σ^* by declaring that $x \sim_L y$ if and only if for all $z \in \Sigma^*$, $xz \in L$ if and only if $yz \in L$.

Theorem (Myhill-Nerode)

The language L is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_L$.

Sketch of proof.

If L is accepted by a finite automaton, then any two words leading to the same state are equivalent. Conversely, if there are finitely many equivalence classes, these correspond to the states of a minimal finite automaton which accepts L. □

Regular functions

Let U be a finite set. Let $f : \Sigma^* \to U$ be a function. Define another equivalence relation on Σ^* by declaring that $x \sim_f y$ if and only if for all $z \in \Sigma^*$, $f(xz) = f(yz)$.

We say that f is *regular* if $f^{-1}(u)$ is a regular language for all $u \in U$. Equivalently, there exist an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to U$ such that $f = h \circ g_\Delta$ (in which case we say that Δ *accepts* f).

Theorem (Myhill-Nerode for functions)

The function f is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_f$.

Sketch of proof.

Similar. □

Regular functions

Let U be a finite set. Let $f : \Sigma^* \to U$ be a function. Define another equivalence relation on Σ^* by declaring that $x \sim_f y$ if and only if for all $z \in \Sigma^*$, $f(xz) = f(yz)$.

We say that f is *regular* if $f^{-1}(u)$ is a regular language for all $u \in U$. Equivalently, there exist an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to U$ such that $f = h \circ g_\Delta$ (in which case we say that Δ *accepts* f).

Theorem (Myhill-Nerode for functions)

The function f is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_f$.

Sketch of proof.

Similar. □

Regular functions

Let U be a finite set. Let $f : \Sigma^* \to U$ be a function. Define another equivalence relation on Σ^* by declaring that $x \sim_f y$ if and only if for all $z \in \Sigma^*$, $f(xz) = f(yz)$.

We say that f is *regular* if $f^{-1}(u)$ is a regular language for all $u \in U$. Equivalently, there exist an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to U$ such that $f = h \circ g_\Delta$ (in which case we say that Δ *accepts* f).

Theorem (Myhill-Nerode for functions)

The function f is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_f$.

Sketch of proof.

Similar. □

Regular functions

Let U be a finite set. Let $f : \Sigma^* \to U$ be a function. Define another equivalence relation on Σ^* by declaring that $x \sim_f y$ if and only if for all $z \in \Sigma^*$, $f(xz) = f(yz)$.

We say that f is *regular* if $f^{-1}(u)$ is a regular language for all $u \in U$. Equivalently, there exist an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to U$ such that $f = h \circ g_\Delta$ (in which case we say that Δ *accepts* f).

Theorem (Myhill-Nerode for functions)

The function f is regular if and only if Σ^* splits into finitely many equivalence classes under $\sim_f$.

Sketch of proof.

Similar. $\square$

Contents

Finite fields

For the remainder of these two talks, fix a prime number $p > 0$ and let q be a power of p. Up to isomorphism, there is a unique finite field of q elements, which we denote by $\mathbb{F}_q$. (This object is not unique up to *unique* isomorphism, but never mind.)

Every finite extension of $\mathbb{F}_q$ is again a finite field, and thus isomorphic to $\mathbb{F}_{q'}$ where q' must be a power of q. Conversely, every power of q as the cardinality of a finite extension of $\mathbb{F}_q$.

For example, we can write

$$\begin{aligned}\mathbb{F}_4 &\cong (\mathbb{Z}/2\mathbb{Z})[z]/(z^2+z+1)\\ \mathbb{F}_9 &\cong (\mathbb{Z}/3\mathbb{Z})]z]/(z^2+1).\end{aligned}$$

Finite fields

For the remainder of these two talks, fix a prime number $p > 0$ and let q be a power of p. Up to isomorphism, there is a unique finite field of q elements, which we denote by $\mathbb{F}_q$. (This object is not unique up to *unique* isomorphism, but never mind.)

Every finite extension of $\mathbb{F}_q$ is again a finite field, and thus isomorphic to $\mathbb{F}_{q'}$ where q' must be a power of q. Conversely, every power of q as the cardinality of a finite extension of $\mathbb{F}_q$.

For example, we can write

$$\mathbb{F}_4 \cong (\mathbb{Z}/2\mathbb{Z})[z]/(z^2 + z + 1)$$
$$\mathbb{F}_9 \cong (\mathbb{Z}/3\mathbb{Z})]z]/(z^2 + 1).$$

Finite fields

For the remainder of these two talks, fix a prime number $p > 0$ and let q be a power of p. Up to isomorphism, there is a unique finite field of q elements, which we denote by $\mathbb{F}_q$. (This object is not unique up to *unique* isomorphism, but never mind.)

Every finite extension of $\mathbb{F}_q$ is again a finite field, and thus isomorphic to $\mathbb{F}_{q'}$ where q' must be a power of q. Conversely, every power of q as the cardinality of a finite extension of $\mathbb{F}_q$.

For example, we can write

$$\mathbb{F}_4 \cong (\mathbb{Z}/2\mathbb{Z})[z]/(z^2 + z + 1)$$
$$\mathbb{F}_9 \cong (\mathbb{Z}/3\mathbb{Z})]z]/(z^2 + 1).$$

Frobenius

Since $\mathbb{F}_q$ is of characteristic p, the *Frobenius map* $x \mapsto x^p$ is a ring homomorphism. It is also injective, so it is in fact a field automorphism.

We will use frequently the fact that the p-th power map also induces a Frobenius endomorphism on $\mathbb{F}_q(t)$ and $\mathbb{F}_q((t))$. These maps are injective but not surjective: an element of $\mathbb{F}_q(t)$ (resp. $\mathbb{F}_q((t))$) is a p-th power if and only if it is a rational function (resp. Laurent series) in t^p.

Frobenius

Since $\mathbb{F}_q$ is of characteristic p, the *Frobenius map* $x \mapsto x^p$ is a ring homomorphism. It is also injective, so it is in fact a field automorphism.

We will use frequently the fact that the p-th power map also induces a Frobenius endomorphism on $\mathbb{F}_q(t)$ and $\mathbb{F}_q((t))$. These maps are injective but not surjective: an element of $\mathbb{F}_q(t)$ (resp. $\mathbb{F}_q((t))$) is a p-th power if and only if it is a rational function (resp. Laurent series) in t^p.

The theorem of Christol

Fix the alphabet $\Sigma = \{0, \dots, p-1\}$. We may identify nonnegative integers with words on Σ using base-p expansions. We will allow arbitrary leading zeroes.

For $f = \sum_{n \in \mathbb{Z}} f_n t^n \in \mathbb{F}_q((t))$, we identify f with a function $f : \Sigma^* \to \mathbb{F}_q$ taking a base-p expansion of n (with any number of leading zeroes) to f_n. We say $f \in \mathbb{F}_q((t))$ is *automatic* if the corresponding function $f : \Sigma^* \to \mathbb{F}_q$ is regular.

Theorem (Christol, 1979; Christol–Kamae–Mendès France–aRauzy, 1980)

A formal Laurent series is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

The theorem of Christol

Fix the alphabet $\Sigma = \{0, \ldots, p-1\}$. We may identify nonnegative integers with words on Σ using base-p expansions. We will allow arbitrary leading zeroes.

For $f = \sum_{n \in \mathbb{Z}} f_n t^n \in \mathbb{F}_q((t))$, we identify f with a function $f : \Sigma^* \to \mathbb{F}_q$ taking a base-p expansion of n (with any number of leading zeroes) to f_n. We say $f \in \mathbb{F}_q((t))$ is *automatic* if the corresponding function $f : \Sigma^* \to \mathbb{F}_q$ is regular.

Theorem (Christol, 1979; Christol–Kamae–Mendès France–aRauzy, 1980)

A formal Laurent series is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

The theorem of Christol

Fix the alphabet $\Sigma = \{0, \ldots, p-1\}$. We may identify nonnegative integers with words on Σ using base-p expansions. We will allow arbitrary leading zeroes.

For $f = \sum_{n \in \mathbb{Z}} f_n t^n \in \mathbb{F}_q((t))$, we identify f with a function $f : \Sigma^* \to \mathbb{F}_q$ taking a base-p expansion of n (with any number of leading zeroes) to f_n. We say $f \in \mathbb{F}_q((t))$ is *automatic* if the corresponding function $f : \Sigma^* \to \mathbb{F}_q$ is regular.

Theorem (Christol, 1979; Christol–Kamae–Mendès France–aRauzy, 1980)

A formal Laurent series is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

Example: the Thue-Morse sequence

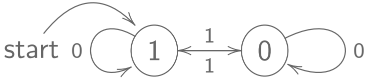
Take $f = \sum_{n=0}^{\infty} f_n t^n \in \mathbb{F}_2((t))$ with

$$f_n = \begin{cases} 1 & \text{if the number of 1's in the base-2 expansion of } n \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Then f is automatic, e.g., for the regular expression

$$0^*(10^*10^*)^*$$

or the DFA



and f is algebraic:

$$(1+t)^3 f^2 + (1+t)^2 f + t = 0.$$

Example: the Thue-Morse sequence

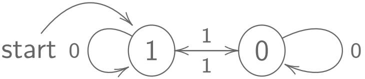
Take $f = \sum_{n=0}^{\infty} f_n t^n \in \mathbb{F}_2((t))$ with

$$f_n = \begin{cases} 1 & \text{if the number of 1's in the base-2 expansion of } n \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Then f is automatic, e.g., for the regular expression

$$0^*(10^*10^*)^*$$

or the DFA



and f is algebraic:

$$(1+t)^3 f^2 + (1+t)^2 f + t = 0.$$

Example: the Thue-Morse sequence

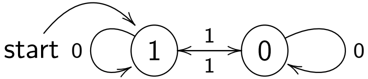
Take $f = \sum_{n=0}^{\infty} f_n t^n \in \mathbb{F}_2((t))$ with

$$f_n = \begin{cases} 1 & \text{if the number of 1's in the base-2 expansion of } n \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Then f is automatic, e.g., for the regular expression

$$0^*(10^*10^*)^*$$

or the DFA



and f is algebraic:

$$(1+t)^3 f^2 + (1+t)^2 f + t = 0.$$

Example: the Thue-Morse sequence

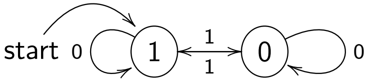
Take $f = \sum_{n=0}^{\infty} f_n t^n \in \mathbb{F}_2((t))$ with

$$f_n = \begin{cases} 1 & \text{if the number of 1's in the base-2 expansion of } n \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Then f is automatic, e.g., for the regular expression

$$0^*(10^*10^*)^*$$

or the DFA



and f is algebraic:

$$(1+t)^3 f^2 + (1+t)^2 f + t = 0.$$

Example: from the Putnam competition

Problem (1989 Putnam competition, problem A6)

Let $\alpha = 1 + a_1 x + a_2 x^2 + \cdots$ *be a formal power series with coefficients in the field of two elements. Let*

$$a_n = \begin{cases} 1 & \text{if every block of zeros in the binary expansion of } n \text{ has an even} \\ & \text{number of zeros in the block} \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\alpha^3 + x\alpha + 1 = 0$.

Application: the Hadamard product

For $f = \sum_{n \in \mathbb{Z}} f_n t^n, g = \sum_{n \in \mathbb{Z}} g_n t^n \in \mathbb{F}_q((t))$, define the *Hadamard product*

$$f \odot g = \sum_{n \in \mathbb{Z}} f_n g_n t^n.$$

Theorem (Furstenberg, 1967)

If $f, g \in \mathbb{F}_q((t))$ are algebraic over $\mathbb{F}_q(t)$, then so is $f \odot g$.

Sketch of proof.

Check the analogous assertion for automatic sequences, which is easy. See Allouche–Shallit, Theorem 12.2.6. □

Note that $\mathbb{F}_q$ is special: over $\mathbb{Q}(t)$, f is algebraic but not $f \odot f$ for

$$f = (1 - 4t)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} t^n.$$

Application: the Hadamard product

For $f = \sum_{n\in\mathbb{Z}} f_n t^n, g = \sum_{n\in\mathbb{Z}} g_n t^n \in \mathbb{F}_q((t))$, define the *Hadamard product*

$$f \odot g = \sum_{n\in\mathbb{Z}} f_n g_n t^n.$$

Theorem (Furstenberg, 1967)

If $f, g \in \mathbb{F}_q((t))$ are algebraic over $\mathbb{F}_q(t)$, then so is $f \odot g$.

Sketch of proof.

Check the analogous assertion for automatic sequences, which is easy. See Allouche–Shallit, Theorem 12.2.6. □

Note that $\mathbb{F}_q$ is special: over $\mathbb{Q}(t)$, f is algebraic but not $f \odot f$ for

$$f = (1-4t)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} t^n.$$

Application: the Hadamard product

For $f = \sum_{n\in\mathbb{Z}} f_n t^n, g = \sum_{n\in\mathbb{Z}} g_n t^n \in \mathbb{F}_q((t))$, define the *Hadamard product*

$$f \odot g = \sum_{n\in\mathbb{Z}} f_n g_n t^n.$$

Theorem (Furstenberg, 1967)

If $f, g \in \mathbb{F}_q((t))$ are algebraic over $\mathbb{F}_q(t)$, then so is $f \odot g$.

Sketch of proof.

Check the analogous assertion for automatic sequences, which is easy. See Allouche–Shallit, Theorem 12.2.6. □

Note that $\mathbb{F}_q$ is special: over $\mathbb{Q}(t)$, f is algebraic but not $f \odot f$ for

$$f = (1-4t)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} t^n.$$

Application: the Hadamard product

For $f = \sum_{n\in\mathbb{Z}} f_n t^n, g = \sum_{n\in\mathbb{Z}} g_n t^n \in \mathbb{F}_q((t))$, define the *Hadamard product*

$$f \odot g = \sum_{n\in\mathbb{Z}} f_n g_n t^n.$$

Theorem (Furstenberg, 1967)

If $f, g \in \mathbb{F}_q((t))$ are algebraic over $\mathbb{F}_q(t)$, then so is $f \odot g$.

Sketch of proof.

Check the analogous assertion for automatic sequences, which is easy. See Allouche–Shallit, Theorem 12.2.6. □

Note that $\mathbb{F}_q$ is special: over $\mathbb{Q}(t)$, f is algebraic but not $f \odot f$ for

$$f = (1-4t)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} t^n.$$

Application: diagonals

Theorem (Furstenberg, 1967 for $f \in \mathbb{F}_q(t,u)$; Deligne, 1984)

Let $f = \sum_{m,n=0}^{\infty} f_{mn} t^m u^n$ be a bivariate formal power series over $\mathbb{F}_q$ which is algebraic over $\mathbb{F}_q(t,u)$. Then the diagonal series $\sum_{n=0}^{\infty} f_{nn} t^n$ is algebraic over $\mathbb{F}_q(t)$.

Proof.

This follows from a multivariate analogue of Christol's theorem. See Allouche–Shallit, Theorem 14.4.2. □

Conversely, every power series algebraic over $\mathbb{F}_q(t)$ arises as the diagonal of some $f \in \mathbb{F}_q(t,u)$ (Furstenberg, 1967). See Allouche-Shallit, Theorem 12.7.3.

Application: diagonals

Theorem (Furstenberg, 1967 for $f \in \mathbb{F}_q(t, u)$; Deligne, 1984)

Let $f = \sum_{m,n=0}^{\infty} f_{mn} t^m u^n$ be a bivariate formal power series over $\mathbb{F}_q$ which is algebraic over $\mathbb{F}_q(t, u)$. Then the diagonal series $\sum_{n=0}^{\infty} f_{nn} t^n$ is algebraic over $\mathbb{F}_q(t)$.

Proof.

This follows from a multivariate analogue of Christol's theorem. See Allouche–Shallit, Theorem 14.4.2. □

Conversely, every power series algebraic over $\mathbb{F}_q(t)$ arises as the diagonal of some $f \in \mathbb{F}_q(t, u)$ (Furstenberg, 1967). See Allouche-Shallit, Theorem 12.7.3.

Application: diagonals

Theorem (Furstenberg, 1967 for $f \in \mathbb{F}_q(t,u)$; Deligne, 1984)

Let $f = \sum_{m,n=0}^{\infty} f_{mn} t^m u^n$ be a bivariate formal power series over $\mathbb{F}_q$ which is algebraic over $\mathbb{F}_q(t,u)$. Then the diagonal series $\sum_{n=0}^{\infty} f_{nn} t^n$ is algebraic over $\mathbb{F}_q(t)$.

Proof.

This follows from a multivariate analogue of Christol's theorem. See Allouche–Shallit, Theorem 14.4.2. □

Conversely, every power series algebraic over $\mathbb{F}_q(t)$ arises as the diagonal of some $f \in \mathbb{F}_q(t,u)$ (Furstenberg, 1967). See Allouche-Shallit, Theorem 12.7.3.

Application: transcendence results

The existence of Christol's theorem makes it possible to prove much better transcendence results over $\mathbb{F}_q(t)$ than over $\mathbb{Q}$.

Theorem (Wade, 1941; Allouche, 1990 using Christol)

The "Carlitz π"

$$\pi_q = \prod_{k=1}^{\infty} \left(1 - \frac{t^{q^k} - t}{t^{q^{k+1}} - t}\right)$$

is transcendental over $\mathbb{F}_q(t)$.

Proof.

See Allouche–Shallit, Theorem 12.4.1. □

Application: transcendence results

The existence of Christol's theorem makes it possible to prove much better transcendence results over $\mathbb{F}_q(t)$ than over $\mathbb{Q}$.

Theorem (Wade, 1941; Allouche, 1990 using Christol)

The "Carlitz π"

$$\pi_q = \prod_{k=1}^{\infty} \left(1 - \frac{t^{q^k} - t}{t^{q^{k+1}} - t}\right)$$

is transcendental over $\mathbb{F}_q(t)$.

Proof.

See Allouche–Shallit, Theorem 12.4.1. □

Application: transcendence results

The existence of Christol's theorem makes it possible to prove much better transcendence results over $\mathbb{F}_q(t)$ than over $\mathbb{Q}$.

Theorem (Wade, 1941; Allouche, 1990 using Christol)

The "Carlitz π"

$$\pi_q = \prod_{k=1}^{\infty} \left(1 - \frac{t^{q^k} - t}{t^{q^{k+1}} - t}\right)$$

is transcendental over $\mathbb{F}_q(t)$.

Proof.

See Allouche–Shallit, Theorem 12.4.1. □

Contents

Algebraicity in characteristic p

Recall that $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if the powers of f all lie in a finite dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$. The following variant (with the same proof) will be useful.

Proposition (Ore)

The element $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if $f, f^p, f^{p^2}, \dots$ all belong to a finite-dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$.

Proof.

If f is a root of a monic polynomial P of degree d over $\mathbb{F}_q(t)$, then every power of f belongs to the $\mathbb{F}_q(t)$-linear span of $1, f, \dots, f^{d-1}$. Conversely, if the inclusion holds, then any linear dependence among $f, f^p, f^{p^2}, \dots$ gives rise to a polynomial over $\mathbb{F}_q(t)$ having f as a root. □

Algebraicity in characteristic p

Recall that $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if the powers of f all lie in a finite dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$. The following variant (with the same proof) will be useful.

Proposition (Ore)

The element $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if $f, f^p, f^{p^2}, \dots$ all belong to a finite-dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$.

Proof.

If f is a root of a monic polynomial P of degree d over $\mathbb{F}_q(t)$, then every power of f belongs to the $\mathbb{F}_q(t)$-linear span of $1, f, \dots, f^{d-1}$. Conversely, if the inclusion holds, then any linear dependence among $f, f^p, f^{p^2}, \dots$ gives rise to a polynomial over $\mathbb{F}_q(t)$ having f as a root. □

Algebraicity in characteristic p

Recall that $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if the powers of f all lie in a finite dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$. The following variant (with the same proof) will be useful.

Proposition (Ore)

The element $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$ if and only if $f, f^p, f^{p^2}, \dots$ all belong to a finite-dimensional $\mathbb{F}_q(t)$-subspace of $\mathbb{F}_q((t))$.

Proof.

If f is a root of a monic polynomial P of degree d over $\mathbb{F}_q(t)$, then every power of f belongs to the $\mathbb{F}_q(t)$-linear span of $1, f, \dots, f^{d-1}$. Conversely, if the inclusion holds, then any linear dependence among $f, f^p, f^{p^2}, \dots$ gives rise to a polynomial over $\mathbb{F}_q(t)$ having f as a root. □

Automatic implies algebraic

Let $f = \sum_{n \in \mathbb{Z}} f_n t^n \in \mathbb{F}_q((t))$ be automatic. Choose an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to \mathbb{F}_q$ such that $f = h \circ g_\Delta$. Define

$$e_s = \sum_{n \geq 0, g_\Delta(n) = s} t^n \qquad (s \in S).$$

Note that

$$f = \sum_{s \in S} h(s) e_s,$$

so it suffices to check that the e_s are algebraic. The key relation is

$$e_s = \sum_{s' \in S, i \in \{0, \dots, p-1\} : \delta(s', i) = s} e_{s'}^p t^i.$$

(This is correct even for $s = s_0$ because we must have $\delta(s_0, 0) = s_0$.)

Automatic implies algebraic

Let $f = \sum_{n \in \mathbb{Z}} f_n t^n \in \mathbb{F}_q((t))$ be automatic. Choose an automaton $\Delta = (S, s_0, \delta)$ and a function $h : S \to \mathbb{F}_q$ such that $f = h \circ g_\Delta$. Define

$$e_s = \sum_{n \geq 0, g_\Delta(n) = s} t^n \qquad (s \in S).$$

Note that

$$f = \sum_{s \in S} h(s) e_s,$$

so it suffices to check that the e_s are algebraic. The key relation is

$$e_s = \sum_{s' \in S, i \in \{0, \dots, p-1\} : \delta(s', i) = s} e_{s'}^p t^i.$$

(This is correct even for $s = s_0$ because we must have $\delta(s_0, 0) = s_0$.)

Automatic implies algebraic (continued)

Since we are in characteristic p, the p-th power map is an automorphism. Hence for each $m \geq 0$,

$$e_s^{p^m} = \sum_{s',i:\delta(s',i)=s} e_{s'}^{p^{m+1}} t^{ip^m}.$$

Therefore $e_s^{p^m}$ is contained in the $\mathbb{F}_q(t)$-span of the $e_{s'}^{p^{m+1}}$.

By induction, $\{e_s^{p^i} : s \in S, i = 0, \ldots, m\}$ is contained in the $\mathbb{F}_q(t)$-span of $\{e_s^{p^m} : s \in S\}$. In particular, $e_s, e_s^p, \ldots, e_s^{p^m}$ belong to an $\mathbb{F}_q(t)$-vector space whose dimension is *bounded independent of m*. It follows that e_s is algebraic, as then is f.

Automatic implies algebraic (continued)

Since we are in characteristic p, the p-th power map is an automorphism. Hence for each $m \geq 0$,

$$e_s^{p^m} = \sum_{s', i: \delta(s', i) = s} e_{s'}^{p^{m+1}} t^{ip^m}.$$

Therefore $e_s^{p^m}$ is contained in the $\mathbb{F}_q(t)$-span of the $e_{s'}^{p^{m+1}}$.

By induction, $\{e_s^{p^i} : s \in S, i = 0, \ldots, m\}$ is contained in the $\mathbb{F}_q(t)$-span of $\{e_s^{p^m} : s \in S\}$. In particular, $e_s, e_s^p, \ldots, e_s^{p^m}$ belong to an $\mathbb{F}_q(t)$-vector space whose dimension is *bounded independent of m*. It follows that e_s is algebraic, as then is f.

Contents

Decimation of power series

The proof in this direction uses a criterion for automaticity analogous to that of algebraicity, except with the p-th power map replaced by some maps in the opposite direction.

Lemma

For $f \in \mathbb{F}_q((t))$, there is a unique way to write

$$f = d_0(f)^p + t d_1(f)^p + \cdots + t^{p-1} d_{p-1}(f)^p$$

with $d_0(f), \ldots, d_{p-1}(f) \in \mathbb{F}_q((t))$.

Proof.

Sort the terms of f by their degree modulo p, then recall that an element of $\mathbb{F}_q((t))$ is a power series in t^p if and only if it is a p-th power. □

Decimation of power series

The proof in this direction uses a criterion for automaticity analogous to that of algebraicity, except with the p-th power map replaced by some maps in the opposite direction.

Lemma

For $f \in \mathbb{F}_q((t))$, there is a unique way to write

$$f = d_0(f)^p + td_1(f)^p + \cdots + t^{p-1}d_{p-1}(f)^p$$

with $d_0(f), \ldots, d_{p-1}(f) \in \mathbb{F}_q((t))$.

Proof.

Sort the terms of f by their degree modulo p, then recall that an element of $\mathbb{F}_q((t))$ is a power series in t^p if and only if it is a p-th power. $\square$

Decimation and automaticity

We view $d_0, \dots, d_{p-1}$ as maps from $\mathbb{F}_q((t))$ to itself. These maps are additive:

$$d_i(f+g) = d_i(f) + d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

but not multiplicative *per se*. Something similar is true, though:

$$d_i(f^p g) = f d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

Using the d_i, we can give a finiteness criterion for automaticity.

Proposition

For $f \in \mathbb{F}_q((t))$, f is automatic if and only if f is contained in a finite subset of $\mathbb{F}_q((t))$ closed under d_i for $i = 0, \dots, p-1$.

Proof.

This is a reformulation of Myhill-Nerode. □

Decimation and automaticity

We view $d_0, \dots, d_{p-1}$ as maps from $\mathbb{F}_q((t))$ to itself. These maps are additive:

$$d_i(f+g) = d_i(f) + d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

but not multiplicative *per se*. Something similar is true, though:

$$d_i(f^p g) = f d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

Using the d_i, we can give a finiteness criterion for automaticity.

Proposition

For $f \in \mathbb{F}_q((t))$, f is automatic if and only if f is contained in a finite subset of $\mathbb{F}_q((t))$ closed under d_i for $i = 0, \dots, p-1$.

Proof.

This is a reformulation of Myhill-Nerode. □

Decimation and automaticity

We view $d_0, \dots, d_{p-1}$ as maps from $\mathbb{F}_q((t))$ to itself. These maps are additive:

$$d_i(f+g) = d_i(f) + d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

but not multiplicative *per se*. Something similar is true, though:

$$d_i(f^p g) = f d_i(g) \qquad (f, g \in \mathbb{F}_q((t))).$$

Using the d_i, we can give a finiteness criterion for automaticity.

Proposition

For $f \in \mathbb{F}_q((t))$, f is automatic if and only if f is contained in a finite subset of $\mathbb{F}_q((t))$ closed under d_i for $i = 0, \dots, p-1$.

Proof.

This is a reformulation of Myhill-Nerode. □

Decimation of rational functions

We define the *degree* of a nonzero rational function $f \in \mathbb{F}_q(t)$ by writing $f = g/h$ with $g, h \in \mathbb{F}_q[t]$ nonzero and coprime, then putting

$$\deg(f) = \max\{\deg(g), \deg(h)\}.$$

By convention, $\deg(0) = -\infty$.

Lemma

For $f \in \mathbb{F}_q(t)$ and $i = 0, \dots, p-1$, we have $d_i(f) \in \mathbb{F}_q(t)$ and $\deg(d_i(f)) \leq \deg(f)$.

Proof.

We have

$$d_i(f) = d_i(gh^{p-1}/h^p) = d_i(gh^{p-1})/h$$

and $\deg(d_i(gh^{p-1})) \leq \deg(gh^{p-1})/p \leq \deg(f)$. □

Decimation of rational functions

We define the *degree* of a nonzero rational function $f \in \mathbb{F}_q(t)$ by writing $f = g/h$ with $g, h \in \mathbb{F}_q[t]$ nonzero and coprime, then putting

$$\deg(f) = \max\{\deg(g), \deg(h)\}.$$

By convention, $\deg(0) = -\infty$.

Lemma

For $f \in \mathbb{F}_q(t)$ and $i = 0, \dots, p-1$, we have $d_i(f) \in \mathbb{F}_q(t)$ and $\deg(d_i(f)) \leq \deg(f)$.

Proof.

We have

$$d_i(f) = d_i(gh^{p-1}/h^p) = d_i(gh^{p-1})/h$$

and $\deg(d_i(gh^{p-1})) \leq \deg(gh^{p-1})/p \leq \deg(f)$. □

Decimation of rational functions

We define the *degree* of a nonzero rational function $f \in \mathbb{F}_q(t)$ by writing $f = g/h$ with $g, h \in \mathbb{F}_q[t]$ nonzero and coprime, then putting

$$\deg(f) = \max\{\deg(g), \deg(h)\}.$$

By convention, $\deg(0) = -\infty$.

Lemma

For $f \in \mathbb{F}_q(t)$ and $i = 0, \dots, p-1$, we have $d_i(f) \in \mathbb{F}_q(t)$ and $\deg(d_i(f)) \leq \deg(f)$.

Proof.

We have

$$d_i(f) = d_i(gh^{p-1}/h^p) = d_i(gh^{p-1})/h$$

and $\deg(d_i(gh^{p-1})) \leq \deg(gh^{p-1})/p \leq \deg(f)$. □

More on algebraicity in characteristic p

Proposition (Ore)

If $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$, then f is in the $\mathbb{F}_q(t)$-span of $f^p, f^{p^2}, \dots$.

Proof.

We have a relation

$$f^{p^l} = h_1 f^{p^{l+1}} + \cdots + h_m f^{p^{l+m}}$$

for some $l, m \geq 0$ and $h_1, \dots, h_m \in \mathbb{F}_q(t)$. If $l > 0$, then also

$$f^{p^{l-1}} = d_0(h_1) f^{p^l} + \cdots + d_0(h_m) f^{p^{l+m-1}},$$

so we may force $l = 0$. □

More on algebraicity in characteristic p

Proposition (Ore)

If $f \in \mathbb{F}_q((t))$ is algebraic over $\mathbb{F}_q(t)$, then f is in the $\mathbb{F}_q(t)$-span of $f^p, f^{p^2}, \dots$.

Proof.

We have a relation

$$f^{p^l} = h_1 f^{p^{l+1}} + \cdots + h_m f^{p^{l+m}}$$

for some $l, m \geq 0$ and $h_1, \dots, h_m \in \mathbb{F}_q(t)$. If $l > 0$, then also

$$f^{p^{l-1}} = d_0(h_1) f^{p^l} + \cdots + d_0(h_m) f^{p^{l+m-1}},$$

so we may force $l = 0$. □

Algebraic implies automatic

Suppose that $f \in \mathbb{F}_q((t))$ is algebraic. We then have

$$f = h_1 f^p + \cdots + h_m f^{p^m}$$

for some $h_1, \dots, h_m \in \mathbb{F}_q(t)$. Put $H = \max_j\{\deg(h_j)\}$ and

$$G = \{g \in \mathbb{F}_q((t)) : g = \sum_{j=0}^{m} e_j f^{p^j}, e_j \in \mathbb{F}_q(t), \deg(e_j) \leq H\}.$$

Each e_j is limited to a finite set, so G is finite. But for $g \in G$ and $i = 0, \dots, p-1$,

$$d_i(g) = d_i\left(\sum_{j=1}^{m}(e_j + e_0 h_j) f^{p^j}\right) = \sum_{j=1}^{m} d_i(e_j + e_0 h_j) f^{p^{j-1}} \in G.$$

Hence f belongs to a finite set closed under the d_i, so is automatic.

Algebraic implies automatic

Suppose that $f \in \mathbb{F}_q((t))$ is algebraic. We then have

$$f = h_1 f^p + \cdots + h_m f^{p^m}$$

for some $h_1, \dots, h_m \in \mathbb{F}_q(t)$. Put $H = \max_j \{\deg(h_j)\}$ and

$$G = \{g \in \mathbb{F}_q((t)) : g = \sum_{j=0}^{m} e_j f^{p^j}, e_j \in \mathbb{F}_q(t), \deg(e_j) \leq H\}.$$

Each e_j is limited to a finite set, so G is finite. But for $g \in G$ and $i = 0, \dots, p-1$,

$$d_i(g) = d_i \left(\sum_{j=1}^{m} (e_j + e_0 h_j) f^{p^j} \right) = \sum_{j=1}^{m} d_i(e_j + e_0 h_j) f^{p^{j-1}} \in G.$$

Hence f belongs to a finite set closed under the d_i, so is automatic.

Contents

Preview of part 2

While Christol's theorem identifies the elements of $\mathbb{F}_q((t))$ which are algebraic over $\mathbb{F}_q(t)$, this is not enough to describe a full algebraic closure of $\mathbb{F}_q(t)$. That is, there are nonconstant polynomials over $\mathbb{F}_q(t)$ with no roots over $\mathbb{F}_q((t))$.

In part 2, we will see how to replace the field $\mathbb{F}_q((t))$ by a field of *generalized power series* so that the analogue of Christol's theorem holds and does determine a full algebraic closure of $\mathbb{F}_q(t)$.

Preview of part 2

While Christol's theorem identifies the elements of $\mathbb{F}_q((t))$ which are algebraic over $\mathbb{F}_q(t)$, this is not enough to describe a full algebraic closure of $\mathbb{F}_q(t)$. That is, there are nonconstant polynomials over $\mathbb{F}_q(t)$ with no roots over $\mathbb{F}_q((t))$.

In part 2, we will see how to replace the field $\mathbb{F}_q((t))$ by a field of *generalized power series* so that the analogue of Christol's theorem holds and does determine a full algebraic closure of $\mathbb{F}_q(t)$.