Christol's theorem and its analogue for generalized power series, part 2

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: K.S. Kedlaya, "Finite automata and algebraic extensions of function fields", *Journal de Théorie des Nombres de Bordeaux* **18** (2006), 379–420.

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

Contents

Recap: Christol's theorem

Theorem (Christol, 1979)

Let $\mathbb{F}_q$ be a finite field of characteristic p. A formal power series

$$f = \sum_{n=0}^{\infty} f_n t^n \in \mathbb{F}_q[\![t]\!]$$

is algebraic over the rational function field $\mathbb{F}_q(t)$ if and only if it is **automatic***: for all $c \in \mathbb{F}_q$, the set of base-p expansions of those $n \geq 0$ with $f_n = c$ form a regular language on the alphabet $\{0, \dots, p-1\}$.*

Why Christol's theorem is not enough

Theorem (Puiseux, 1850 for $K = \mathbb{C}$)

For K a field of characteristic 0, every finite extension of the field $K((t))$ is contained in some extension of the form $L((t^{1/m}))$ for L a finite extension of K and m a positive integer.

This fails in positive characteristic as noted by Chevalley.

Proposition

The polynomial

$$z^p - z - t^{-1} \in \mathbb{F}_q((t))[z]$$

has no root in $\mathbb{F}_{q'}((t^{1/m}))$ for any power q' of q and any positive integer m. (Proof on next slide.)

Why Christol's theorem is not enough (continued)

Proof of the Proposition.

Suppose $z = \sum_n z_n t^n$ were such a root. Then

$$z^p = \sum_n z_n^p t^{np} = \sum_n z_{n/p}^p t^n$$

and so

$$t^{-1} = \sum_n (z_{n/p}^p - z_n) t^n.$$

Since z is a (nonzero) formal power series in $t^{1/m}$ for some m, there must be a smallest index i for which $z_i \neq 0$. If $i < -1/p$, then $0 = z_i^p - z_{pi}$ and so $z_{pi} \neq 0$, contradiction. Therefore $z_{-1} = 0$, which forces

$$1 = z_{-1/p} = z_{-1/p^2} = \cdots$$

and precludes $z \in \mathbb{F}_{q'}((t^{1/m}))$ for any m, contradiction. □

Contents

Generalized power series

Definition (Hahn, 1905)

A *generalized power series* over a field K is a formal expression $f = \sum_{n \in \mathbb{Q}} f_n t^n$ with $f_n \in K$ whose *support*

$$\mathrm{Supp}(f) = \{n \in \mathbb{Q} : f_n \neq 0\}$$

is a **well-ordered** subset of $\mathbb{Q}$, i.e., one containing no infinite decreasing sequence. (Equivalently, every nonempty subset has a least element.)

We will write $K((t^{\mathbb{Q}}))$ for the set of generalized power series. To be precise, these are really generalized Laurent series; we write $K[\![t^{\mathbb{Q}}]\!]$ to pick out those series whose supports are contained in $[0, +\infty)$.

Variants: Hahn allows $\mathbb{Q}$ to be replaced by a totally ordered abelian group. There is even a noncommutative version due to Mal'cev and Neumann (independently).

Generalized power series

Definition (Hahn, 1905)

A *generalized power series* over a field K is a formal expression $f = \sum_{n \in \mathbb{Q}} f_n t^n$ with $f_n \in K$ whose *support*

$$\mathrm{Supp}(f) = \{n \in \mathbb{Q} : f_n \neq 0\}$$

is a **well-ordered** subset of $\mathbb{Q}$, i.e., one containing no infinite decreasing sequence. (Equivalently, every nonempty subset has a least element.)

We will write $K((t^{\mathbb{Q}}))$ for the set of generalized power series. To be precise, these are really generalized Laurent series; we write $K[\![t^{\mathbb{Q}}]\!]$ to pick out those series whose supports are contained in $[0, +\infty)$.

Variants: Hahn allows $\mathbb{Q}$ to be replaced by a totally ordered abelian group. There is even a noncommutative version due to Mal'cev and Neumann (independently).

Generalized power series

Definition (Hahn, 1905)

A *generalized power series* over a field K is a formal expression $f = \sum_{n \in \mathbb{Q}} f_n t^n$ with $f_n \in K$ whose *support*

$$\mathrm{Supp}(f) = \{n \in \mathbb{Q} : f_n \neq 0\}$$

is a **well-ordered** subset of $\mathbb{Q}$, i.e., one containing no infinite decreasing sequence. (Equivalently, every nonempty subset has a least element.)

We will write $K((t^{\mathbb{Q}}))$ for the set of generalized power series. To be precise, these are really generalized Laurent series; we write $K[\![t^{\mathbb{Q}}]\!]$ to pick out those series whose supports are contained in $[0, +\infty)$.

Variants: Hahn allows $\mathbb{Q}$ to be replaced by a totally ordered abelian group. There is even a noncommutative version due to Mal'cev and Neumann (independently).

Arithmetic for generalized power series

It is easy to see that generalized power series can be added formally: the point is that the union of two well-ordered sets is again well-ordered.

Multiplication is less clear: given $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n$, note first that for any $n \in \mathbb{Q}$ the formal sum

$$\sum_{i,j \in \mathbb{Q}: i+j=n} f_i g_j$$

only contains finitely many nonzero terms. Then check that the support of

$$f + g = \sum_{n \in \mathbb{Q}} \left(\sum_{i,j \in \mathbb{Q}: i+j=n} f_i g_j \right) t^n$$

is well-ordered.

Arithmetic for generalized power series

It is easy to see that generalized power series can be added formally: the point is that the union of two well-ordered sets is again well-ordered.

Multiplication is less clear: given $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n$, note first that for any $n \in \mathbb{Q}$ the formal sum

$$\sum_{i,j \in \mathbb{Q}: i+j=n} f_i g_j$$

only contains finitely many nonzero terms. Then check that the support of

$$f + g = \sum_{n \in \mathbb{Q}} \left(\sum_{i,j \in \mathbb{Q}: i+j=n} f_i g_j \right) t^n$$

is well-ordered.

Arithmetic for generalized power series (continued)

It follows that $K[\![t^{\mathbb{Q}}]\!]$ and $K((t^{\mathbb{Q}}))$ are both rings under formal addition and multiplication. The ring $K((t^{\mathbb{Q}}))$ is also a field: any nonzero element can be written as $at^m(1-f)$ where $a \in K^*$, $m \in \mathbb{Q}$, $f \in K[\![t^{\mathbb{Q}}]\!]$, and $f_0 = 0$. But then the sum

$$\sum_{n=0}^{\infty} f^n$$

makes sense and defines an inverse of $1 - f$.

What "the sum makes sense" really means here is that $K((t^{\mathbb{Q}}))$ is complete for the t-adic valuation

$$v_t(f) = \min \operatorname{Supp}(f).$$

Arithmetic for generalized power series (continued)

It follows that $K[\![t^{\mathbb{Q}}]\!]$ and $K((t^{\mathbb{Q}}))$ are both rings under formal addition and multiplication. The ring $K((t^{\mathbb{Q}}))$ is also a field: any nonzero element can be written as $at^m(1-f)$ where $a \in K^*$, $m \in \mathbb{Q}$, $f \in K[\![t^{\mathbb{Q}}]\!]$, and $f_0 = 0$. But then the sum

$$\sum_{n=0}^{\infty} f^n$$

makes sense and defines an inverse of $1 - f$.

What "the sum makes sense" really means here is that $K((t^{\mathbb{Q}}))$ is complete for the t-adic valuation

$$v_t(f) = \min \operatorname{Supp}(f).$$

Algebraic closures

Theorem (Hahn, 1905)

If K is an algebraically closed field, then so is $K((t^{\mathbb{Q}}))$.

Sketch of proof.

Given a nonconstant polynomial P over $K((t^{\mathbb{Q}}))$, one can build a root by a *transfinite* sequence of successive approximations (one indexed by some countable ordinal). $\square$

In particular, if K is an algebraic closure of $\mathbb{F}_q$, then $K((t^{\mathbb{Q}}))$ contains an algebraic closure of $\mathbb{F}_q(t)$. Our goal (inspired by a suggestion of Abhyankar) is to identify this algebraic closure explicitly.

More on algebraic closures

Let $\mathbb{Z}[p^{-1}]$ denote the subring of $\mathbb{Q}$ generated by p^{-1}, i.e., the ring of rational numbers with only powers of p in their denominators.

Proposition (easy)

Let K be an algebraic closure of $\mathbb{F}_q$. Then every element f of the algebraic closure of $\mathbb{F}_q((t))$ within $\mathbb{F}_q((t^{\mathbb{Q}}))$ has the following properties.

(a) *We have $\mathrm{Supp}(f) \subset m^{-1}\mathbb{Z}[p^{-1}]$ for some positive integer m coprime to p (depending on f).*

(b) *The coefficients of f belong to some finite subfield $\mathbb{F}_{q'}$ of K.*

The same is then true of the algebraic closure of $\mathbb{F}_q(t)$ within $\mathbb{F}_q((t^{\mathbb{Q}}))$.

Contents

Comments on base-p expansions

Elements of $\mathbb{Q}_{\geq 0}$ have well-defined base-p expansions, but only elements of $\mathbb{Z}[p^{-1}]_{\geq 0}$ have finite expansions. Such expansions are words on the alphabet $\{0, \dots, p-1, .\}$, where the last symbol is the *radix point*.

We will allow arbitrary leading and trailing zeroes, but we will insist that to be *valid*, expansions must have exactly one radix point.

Warning: this is a different convention than in the paper (where no leading or trailing zeroes are allowed), but the results are equivalent.

Comments on base-p expansions

Elements of $\mathbb{Q}_{\geq 0}$ have well-defined base-p expansions, but only elements of $\mathbb{Z}[p^{-1}]_{\geq 0}$ have finite expansions. Such expansions are words on the alphabet $\{0, \ldots, p-1, .\}$, where the last symbol is the *radix point*.

We will allow arbitrary leading and trailing zeroes, but we will insist that to be *valid*, expansions must have exactly one radix point.

Warning: this is a different convention than in the paper (where no leading or trailing zeroes are allowed), but the results are equivalent.

Comments on base-p expansions

Elements of $\mathbb{Q}_{\geq 0}$ have well-defined base-p expansions, but only elements of $\mathbb{Z}[p^{-1}]_{\geq 0}$ have finite expansions. Such expansions are words on the alphabet $\{0, \ldots, p-1, .\}$, where the last symbol is the *radix point*.

We will allow arbitrary leading and trailing zeroes, but we will insist that to be *valid*, expansions must have exactly one radix point.

Warning: this is a different convention than in the paper (where no leading or trailing zeroes are allowed), but the results are equivalent.

Automatic generalized power series

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$. We say that f is *automatic* if the function $n \mapsto f_n$ is induced by some finite automaton on the alphabet $\{0, \dots, p-1, .\}$ by identifying n with its base-p expansion.

Lemma (relatively easy)

For m a positive integer and $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$, $\sum_n f_n t^n$ is automatic if and only if $\sum_n f_n t^{mn+a}$ is.

For a general $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$, we say that f is *automatic* if there exist a positive integer m and some $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$ such that $\sum_n f_n t^{mn+a}$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$ and is automatic in the above sense. By the lemma, this specializes back to the previous definition. (In the paper, the second condition is called *quasi-automatic*.)

Automatic generalized power series

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$. We say that f is *automatic* if the function $n \mapsto f_n$ is induced by some finite automaton on the alphabet $\{0, \dots, p-1, .\}$ by identifying n with its base-p expansion.

Lemma (relatively easy)

For m a positive integer and $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$, $\sum_n f_n t^n$ is automatic if and only if $\sum_n f_n t^{mn+a}$ is.

For a general $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$, we say that f is *automatic* if there exist a positive integer m and some $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$ such that $\sum_n f_n t^{mn+a}$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$ and is automatic in the above sense. By the lemma, this specializes back to the previous definition. (In the paper, the second condition is called *quasi-automatic*.)

Automatic generalized power series

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$. We say that f is *automatic* if the function $n \mapsto f_n$ is induced by some finite automaton on the alphabet $\{0, \dots, p-1, .\}$ by identifying n with its base-p expansion.

Lemma (relatively easy)

For m a positive integer and $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$, $\sum_n f_n t^n$ is automatic if and only if $\sum_n f_n t^{mn+a}$ is.

For a general $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$, we say that f is *automatic* if there exist a positive integer m and some $a \in \mathbb{Z}[p^{-1}]_{\geq 0}$ such that $\sum_n f_n t^{mn+a}$ has support in $\mathbb{Z}[p^{-1}]_{\geq 0}$ and is automatic in the above sense. By the lemma, this specializes back to the previous definition. (In the paper, the second condition is called *quasi-automatic*.)

Constraints on automata

For any automatic $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ with support in $\mathbb{Z}[p^{-1}]_{\geq 0}$, the function $f : \mathbb{Z}[p^{-1}]_{\geq 0} \to \mathbb{F}_q$ has the form $h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. We may also ensure that $h \circ g_\Delta$ sends all invalid strings to 0 and is constant over all expansions of a given n (with varying leading and trailing zeroes).

But the converse fails: such data do not in general define a generalized power series! The trouble is that $\mathrm{Supp}(h \circ g_\Delta)$ is usually not well-ordered.

However, one can interpret the condition that $\mathrm{Supp}(h \circ g_\Delta)$ be well-ordered in graph-theoretical terms. See next slide.

Constraints on automata

For any automatic $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ with support in $\mathbb{Z}[p^{-1}]_{\geq 0}$, the function $f : \mathbb{Z}[p^{-1}]_{\geq 0} \to \mathbb{F}_q$ has the form $h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. We may also ensure that $h \circ g_\Delta$ sends all invalid strings to 0 and is constant over all expansions of a given n (with varying leading and trailing zeroes).

But the converse fails: such data do not in general define a generalized power series! The trouble is that $\mathrm{Supp}(h \circ g_\Delta)$ is usually not well-ordered.

However, one can interpret the condition that $\mathrm{Supp}(h \circ g_\Delta)$ be well-ordered in graph-theoretical terms. See next slide.

Constraints on automata

For any automatic $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ with support in $\mathbb{Z}[p^{-1}]_{\geq 0}$, the function $f : \mathbb{Z}[p^{-1}]_{\geq 0} \to \mathbb{F}_q$ has the form $h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. We may also ensure that $h \circ g_\Delta$ sends all invalid strings to 0 and is constant over all expansions of a given n (with varying leading and trailing zeroes).

But the converse fails: such data do not in general define a generalized power series! The trouble is that $\mathrm{Supp}(h \circ g_\Delta)$ is usually not well-ordered.

However, one can interpret the condition that $\mathrm{Supp}(h \circ g_\Delta)$ be well-ordered in graph-theoretical terms. See next slide.

Graph-theoretic constraints

Form the directed multigraph $\tilde{\Gamma}$ on S with an edge from s to s' labeled i whenever $\delta(s, i) = s'$. We say a vertex or edge is *essential* if it occurs along a path from s_0 to a state in $h^{-1}(0)$, otherwise *inessential*.

Let Γ be obtained from $\tilde{\Gamma}$ by removing all inessential vertices and edges. Each state in Γ can be described as *preradix* and *postradix* depending on whether it occurs before or after a radix point along some (hence any) path from s_0. Every state in $h^{-1}(0)$ is postradix.

For $\mathrm{Supp}(f)$ to be well-ordered, it is necessary and sufficient that for each postradix state $s \in \Gamma$,

- there is at most one directed cycle passing through s;
- if so, then the edge on this cycle from s has a larger label than any other edge from s.

Graph-theoretic constraints

Form the directed multigraph $\tilde{\Gamma}$ on S with an edge from s to s' labeled i whenever $\delta(s,i) = s'$. We say a vertex or edge is *essential* if it occurs along a path from s_0 to a state in $h^{-1}(0)$, otherwise *inessential*.

Let Γ be obtained from $\tilde{\Gamma}$ by removing all inessential vertices and edges. Each state in Γ can be described as *preradix* and *postradix* depending on whether it occurs before or after a radix point along some (hence any) path from s_0. Every state in $h^{-1}(0)$ is postradix.

For $\mathrm{Supp}(f)$ to be well-ordered, it is necessary and sufficient that for each postradix state $s \in \Gamma$,

- there is at most one directed cycle passing through s;
- if so, then the edge on this cycle from s has a larger label than any other edge from s.

Graph-theoretic constraints

Form the directed multigraph $\tilde{\Gamma}$ on S with an edge from s to s' labeled i whenever $\delta(s, i) = s'$. We say a vertex or edge is *essential* if it occurs along a path from s_0 to a state in $h^{-1}(0)$, otherwise *inessential*.

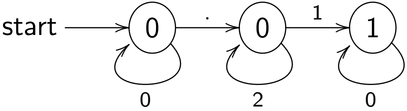
Let Γ be obtained from $\tilde{\Gamma}$ by removing all inessential vertices and edges. Each state in Γ can be described as *preradix* and *postradix* depending on whether it occurs before or after a radix point along some (hence any) path from s_0. Every state in $h^{-1}(0)$ is postradix.

For $\mathrm{Supp}(f)$ to be well-ordered, it is necessary and sufficient that for each postradix state $s \in \Gamma$,

- there is at most one directed cycle passing through s;
- if so, then the edge on this cycle from s has a larger label than any other edge from s.

An example

Take $p = 3$. All unlabeled transitions map to a dummy state labeled 0 which only transitions to itself (and is hence inessential).



In base 3, the support consists of

$$.1, .21, .221, \ldots$$

(omitting leading and trailing zeroes). If the 1 and 2 were reversed we would instead get a decreasing sequence

$$.2, .12, .112, \ldots.$$

An extension of Christol's theorem

Theorem (Kedlaya, 2006)

An element $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

Some sample corollaries:

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n \in \mathbb{F}_q((t^{\mathbb{Q}}))$ are algebraic over $\mathbb{F}_q(t)$, then so is the Hadamard product $f \odot g = \sum_{n \in \mathbb{Q}} f_n g_n t^n$.

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n$ is algebraic over $\mathbb{F}_q(t)$, then so is $\sum_{n \in \mathbb{Q} \cap I} f_n t^n$ for any interval I in $\mathbb{R}$.

An extension of Christol's theorem

Theorem (Kedlaya, 2006)

An element $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

Some sample corollaries:

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n \in \mathbb{F}_q((t^{\mathbb{Q}}))$ are algebraic over $\mathbb{F}_q(t)$, then so is the Hadamard product $f \odot g = \sum_{n \in \mathbb{Q}} f_n g_n t^n$.

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n$ is algebraic over $\mathbb{F}_q(t)$, then so is $\sum_{n \in \mathbb{Q} \cap I} f_n t^n$ for any interval I in $\mathbb{R}$.

An extension of Christol's theorem

Theorem (Kedlaya, 2006)

An element $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

Some sample corollaries:

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n \in \mathbb{F}_q((t^{\mathbb{Q}}))$ are algebraic over $\mathbb{F}_q(t)$, then so is the Hadamard product $f \odot g = \sum_{n \in \mathbb{Q}} f_n g_n t^n$.

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n$ is algebraic over $\mathbb{F}_q(t)$, then so is $\sum_{n \in \mathbb{Q} \cap I} f_n t^n$ for any interval I in $\mathbb{R}$.

An extension of Christol's theorem

Theorem (Kedlaya, 2006)

An element $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if it is automatic.

Some sample corollaries:

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n, g = \sum_{n \in \mathbb{Q}} g_n t^n \in \mathbb{F}_q((t^{\mathbb{Q}}))$ are algebraic over $\mathbb{F}_q(t)$, then so is the Hadamard product $f \odot g = \sum_{n \in \mathbb{Q}} f_n g_n t^n$.

Corollary

If $f = \sum_{n \in \mathbb{Q}} f_n t^n$ is algebraic over $\mathbb{F}_q(t)$, then so is $\sum_{n \in \mathbb{Q} \cap I} f_n t^n$ for any interval I in $\mathbb{R}$.

The example of Chevalley

The polynomial

$$z^p - z - t^{-1}$$

over $\mathbb{F}_q(t)$ has in $\mathbb{F}_q((t^{\mathbb{Q}}))$ the root

$$f = t^{-1/p} + t^{-1/p^2} + t^{-1/p^3} + \cdots .$$

Note that tf has support in $\mathbb{Z}[p^{-1}]$ which is accepted by the regular expression

$$0^*.@^*0^*$$

where @ represents the digit $p-1$. Hence f is automatic.

Contents

Automatic implies algebraic

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is automatic. To check that f is algebraic, we may assume $\mathrm{Supp}(f) \subset \mathbb{Z}[p^{-1}]_{\geq 0}$. Write $f = h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. Put

$$e_s = \sum_{n \in \mathbb{Z}, g_\Delta(n) = s} t^n, \qquad g_s = \sum_{n \in \mathbb{Z}[p^{-1}] \cap [0,1), g_\Delta(n) = s} t^n.$$

Note that $e_s \neq 0$ (resp. $g_s \neq 0$) only if s is essential and preradix (resp. postradix). Moreover, $f = \sum_s e_s g_{\delta(s,.)}$ and

$$e_s = \sum_{s', i : \delta(s', i) = s} e_{s'}^p t^i, \qquad g_s = \sum_{i=0}^{p-1} g_{\delta(s,i)}^{1/p} t^{i/p}.$$

For $m \geq 0$, $g_s^{p^m}$ belongs to the $\mathbb{F}_q(t)$-span of the g_s, so the g_s are algebraic. Similarly (as before) the e_s are algebraic. Hence f is algebraic.

Automatic implies algebraic

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is automatic. To check that f is algebraic, we may assume $\mathrm{Supp}(f) \subset \mathbb{Z}[p^{-1}]_{\geq 0}$. Write $f = h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. Put

$$e_s = \sum_{n \in \mathbb{Z}, g_\Delta(n) = s} t^n, \qquad g_s = \sum_{n \in \mathbb{Z}[p^{-1}] \cap [0,1), g_\Delta(n) = s} t^n.$$

Note that $e_s \neq 0$ (resp. $g_s \neq 0$) only if s is essential and preradix (resp. postradix). Moreover, $f = \sum_s e_s g_{\delta(s,.)}$ and

$$e_s = \sum_{s', i : \delta(s', i) = s} e_{s'}^p t^i, \qquad g_s = \sum_{i=0}^{p-1} g_{\delta(s,i)}^{1/p} t^{i/p}.$$

For $m \geq 0$, $g_s^{p^m}$ belongs to the $\mathbb{F}_q(t)$-span of the g_s, so the g_s are algebraic. Similarly (as before) the e_s are algebraic. Hence f is algebraic.

Automatic implies algebraic

Suppose $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is automatic. To check that f is algebraic, we may assume $\mathrm{Supp}(f) \subset \mathbb{Z}[p^{-1}]_{\geq 0}$. Write $f = h \circ g_\Delta$ for some finite automaton $\Delta = (S, s_0, \delta)$ and some function $h : S \to \mathbb{F}_q$. Put

$$e_s = \sum_{n \in \mathbb{Z}, g_\Delta(n) = s} t^n, \qquad g_s = \sum_{n \in \mathbb{Z}[p^{-1}] \cap [0,1), g_\Delta(n) = s} t^n.$$

Note that $e_s \neq 0$ (resp. $g_s \neq 0$) only if s is essential and preradix (resp. postradix). Moreover, $f = \sum_s e_s g_{\delta(s,.)}$ and

$$e_s = \sum_{s', i : \delta(s', i) = s} e_{s'}^p t^i, \qquad g_s = \sum_{i=0}^{p-1} g_{\delta(s,i)}^{1/p} t^{i/p}.$$

For $m \geq 0$, $g_s^{p^m}$ belongs to the $\mathbb{F}_q(t)$-span of the g_s, so the g_s are algebraic. Similarly (as before) the e_s are algebraic. Hence f is algebraic.

Automaticity and arithmetic operations

For "algebraic implies automatic," we can't use decimations because Frobenius is bijective on $\mathbb{F}_q((t^{\mathbb{Q}}))$. Instead, we use field theory.

Lemma

The set of automatic elements of $\mathbb{F}_q((t^{\mathbb{Q}}))$ is a subfield.

Sketch of proof.

We check that automatic elements form a subring using some explicit constructions of automata. For $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ nonzero automatic, we know f is algebraic:

$$f^d + h_{d-1}f^{d-1} + \cdots + h_0 = 0$$

for some $h_0, \ldots, h_{d-1} \in \mathbb{F}_q(t)$ with $h_0 \neq 0$. Then

$$f^{-1} = -h_0^{-1}(f^{d-1} + h_{d-1}f^{d-2} + \cdots + h_1)$$

belongs to the subring of automatic elements, which is thus a subfield. □

Automaticity and arithmetic operations

For "algebraic implies automatic," we can't use decimations because Frobenius is bijective on $\mathbb{F}_q((t^{\mathbb{Q}}))$. Instead, we use field theory.

Lemma

The set of automatic elements of $\mathbb{F}_q((t^{\mathbb{Q}}))$ is a subfield.

Sketch of proof.

We check that automatic elements form a subring using some explicit constructions of automata. For $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ nonzero automatic, we know f is algebraic:

$$f^d + h_{d-1} f^{d-1} + \cdots + h_0 = 0$$

for some $h_0, \ldots, h_{d-1} \in \mathbb{F}_q(t)$ with $h_0 \neq 0$. Then

$$f^{-1} = -h_0^{-1}(f^{d-1} + h_{d-1} f^{d-2} + \cdots + h_1)$$

belongs to the subring of automatic elements, which is thus a subfield. □

Automaticity and arithmetic operations

For "algebraic implies automatic," we can't use decimations because Frobenius is bijective on $\mathbb{F}_q((t^{\mathbb{Q}}))$. Instead, we use field theory.

Lemma

The set of automatic elements of $\mathbb{F}_q((t^{\mathbb{Q}}))$ is a subfield.

Sketch of proof.

We check that automatic elements form a subring using some explicit constructions of automata. For $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ nonzero automatic, we know f is algebraic:

$$f^d + h_{d-1} f^{d-1} + \cdots + h_0 = 0$$

for some $h_0, \dots, h_{d-1} \in \mathbb{F}_q(t)$ with $h_0 \neq 0$. Then

$$f^{-1} = -h_0^{-1}(f^{d-1} + h_{d-1} f^{d-2} + \cdots + h_1)$$

belongs to the subring of automatic elements, which is thus a subfield. $\square$

Input from field theory: Artin-Schreier extensions

Lemma (standard)

Let F be a field of characteristic p. Then the $\mathbb{Z}/p\mathbb{Z}$-extensions of F coincide with the **Artin-Schreier extensions***, i.e., those generated by roots of polynomials of the form*

$$z^p - z - c \qquad (c \in F).$$

Note that the Galois action is generated by $z \mapsto z + 1$.

Proposition (standard)

Let K be a finite extension of $\mathbb{F}_q(t)$. Then there exist a power q' of q, a positive integer m, and a finite extension L of $\mathbb{F}_{q'}(t^{1/m})$ containing K such that $L/\mathbb{F}_q(t)$ can be written as a tower of Artin-Schreier field extensions.

Automaticity and Artin-Schreier extensions

Lemma

If $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is automatic and

$$g^p - g = f,$$

then g is automatic.

Sketch of proof.

We may separate the cases where f is supported in $(-\infty, 0)$ and $(0, \infty)$. In these cases we have respectively

$$g = c + f^{-1/p} + f^{-1/p^2} + \cdots$$
$$g = c - f - f^p - \cdots$$

for some $c \in \mathbb{F}_p$. In both cases, we may explicitly construct an automaton producing g from one that produces f. □

Automaticity and Artin-Schreier extensions

Lemma

If $f \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is automatic and

$$g^p - g = f,$$

then g is automatic.

Sketch of proof.

We may separate the cases where f is supported in $(-\infty, 0)$ and $(0, \infty)$. In these cases we have respectively

$$g = c + f^{-1/p} + f^{-1/p^2} + \cdots$$
$$g = c - f - f^p - \cdots$$

for some $c \in \mathbb{F}_p$. In both cases, we may explicitly construct an automaton producing g from one that produces f. □

Algebraicity implies automaticity

We now know that for K an algebraic closure of $\mathbb{F}_q$,

- for q' varying over powers of q, the automatic elements of $\bigcup_{q'} \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ form a subfield of the algebraic closure of $\mathbb{F}_q(t)$ in $K((t^{\mathbb{Q}}))$;
- this subfield contains $\mathbb{F}_{q'}(t^{1/m})$ for any power q' of q and any positive integer m;
- this subfield is closed under extraction of roots of Artin-Schreier polynomials.

It therefore is the whole algebraic closure of $\mathbb{F}_q(t)$. The theorem follows.

Algebraicity implies automaticity

We now know that for K an algebraic closure of $\mathbb{F}_q$,

- for q' varying over powers of q, the automatic elements of $\bigcup_{q'} \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ form a subfield of the algebraic closure of $\mathbb{F}_q(t)$ in $K((t^{\mathbb{Q}}))$;
- this subfield contains $\mathbb{F}_{q'}(t^{1/m})$ for any power q' of q and any positive integer m;
- this subfield is closed under extraction of roots of Artin-Schreier polynomials.

It therefore is the whole algebraic closure of $\mathbb{F}_q(t)$. The theorem follows.

Algebraicity implies automaticity

We now know that for K an algebraic closure of $\mathbb{F}_q$,

- for q' varying over powers of q, the automatic elements of $\bigcup_{q'} \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ form a subfield of the algebraic closure of $\mathbb{F}_q(t)$ in $K((t^{\mathbb{Q}}))$;
- this subfield contains $\mathbb{F}_{q'}(t^{1/m})$ for any power q' of q and any positive integer m;
- this subfield is closed under extraction of roots of Artin-Schreier polynomials.

It therefore is the whole algebraic closure of $\mathbb{F}_q(t)$. The theorem follows.

Algebraicity implies automaticity

We now know that for K an algebraic closure of $\mathbb{F}_q$,

- for q' varying over powers of q, the automatic elements of $\bigcup_{q'} \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ form a subfield of the algebraic closure of $\mathbb{F}_q(t)$ in $K((t^{\mathbb{Q}}))$;
- this subfield contains $\mathbb{F}_{q'}(t^{1/m})$ for any power q' of q and any positive integer m;
- this subfield is closed under extraction of roots of Artin-Schreier polynomials.

It therefore is the whole algebraic closure of $\mathbb{F}_q(t)$. The theorem follows.

Algebraicity implies automaticity

We now know that for K an algebraic closure of $\mathbb{F}_q$,

- for q' varying over powers of q, the automatic elements of $\bigcup_{q'} \mathbb{F}_{q'}((t^{\mathbb{Q}}))$ form a subfield of the algebraic closure of $\mathbb{F}_q(t)$ in $K((t^{\mathbb{Q}}))$;
- this subfield contains $\mathbb{F}_{q'}(t^{1/m})$ for any power q' of q and any positive integer m;
- this subfield is closed under extraction of roots of Artin-Schreier polynomials.

It therefore is the whole algebraic closure of $\mathbb{F}_q(t)$. The theorem follows.

Contents

Automata and explicit computations

When making machine computations in an algebraic closure of $\mathbb{Q}$, it is often inefficient to work exactly because one is forced to keep track of algebraic number fields of large degree. It is sometimes more practical to keep track of approximations in $\mathbb{C}$ of sufficient accuracy, i.e., to do *interval arithmetic*.

It should be possible to similarly compute in an algebraic closure of $\mathbb{F}_q(t)$ using automata. The tricky part is to describe a sensible notion of *approximation*; this is needed because exact computation is usually infeasible.

Automata and explicit computations

When making machine computations in an algebraic closure of $\mathbb{Q}$, it is often inefficient to work exactly because one is forced to keep track of algebraic number fields of large degree. It is sometimes more practical to keep track of approximations in $\mathbb{C}$ of sufficient accuracy, i.e., to do *interval arithmetic*.

It should be possible to similarly compute in an algebraic closure of $\mathbb{F}_q(t)$ using automata. The tricky part is to describe a sensible notion of *approximation*; this is needed because exact computation is usually infeasible.

Relative algebraicity

For K an algebraic closure of $\mathbb{F}_q$, it makes sense to ask whether $x_1, \dots, x_n \in K((t^{\mathbb{Q}}))$ are *algebraically dependent* over $\mathbb{F}_q(t)$, i.e., whether $P(x_1, \dots, x_n) = 0$ for some nonzero n-variate polynomial P over $\mathbb{F}_q(t)$.

Problem

Is there an automata-theoretic characterization of algebraic dependence?

Already the case of ordinary power series is of interest.

Relative algebraicity

For K an algebraic closure of $\mathbb{F}_q$, it makes sense to ask whether $x_1, \dots, x_n \in K((t^{\mathbb{Q}}))$ are *algebraically dependent* over $\mathbb{F}_q(t)$, i.e., whether $P(x_1, \dots, x_n) = 0$ for some nonzero n-variate polynomial P over $\mathbb{F}_q(t)$.

Problem

Is there an automata-theoretic characterization of algebraic dependence?

Already the case of ordinary power series is of interest.