Journal de Théorie des Nombres
de Bordeaux **18** (2006), 379–420

Finite automata and algebraic extensions of function fields

par Kiran S. KEDLAYA

Résumé. On donne une description, dans le langage des automates finis, de la clôture algébrique du corps des fonctions rationnelles $\mathbb{F}_q(t)$ sur un corps fini $\mathbb{F}_q$. Cette description, qui généralise un résultat de Christol, emploie le corps de Hahn-Mal'cev-Neumann des "séries formelles généralisées" sur $\mathbb{F}_q$. En passant, on obtient une caractérisation des ensembles bien ordonnés de nombres rationnels dont les représentations p-adiques sont générées par un automate fini, et on présente des techniques pour calculer dans la clôture algébrique; ces techniques incluent une version en caractéristique non nulle de l'algorithme de Newton-Puiseux pour déterminer les développements locaux des courbes planes. On conjecture une généralisation de nos résultats au cas de plusieurs variables.

Abstract. We give an automata-theoretic description of the algebraic closure of the rational function field $\mathbb{F}_q(t)$ over a finite field $\mathbb{F}_q$, generalizing a result of Christol. The description occurs within the Hahn-Mal'cev-Neumann field of "generalized power series" over $\mathbb{F}_q$. In passing, we obtain a characterization of well-ordered sets of rational numbers whose base p expansions are generated by a finite automaton, and exhibit some techniques for computing in the algebraic closure; these include an adaptation to positive characteristic of Newton's algorithm for finding local expansions of plane curves. We also conjecture a generalization of our results to several variables.

1. Introduction

1.1. Christol's theorem, and its limits. Let $\mathbb{F}_q$ be a finite field of characteristic p, and let $\mathbb{F}_q(t)$ and $\mathbb{F}_q((t))$ denote the fields of rational functions and of formal (Laurent) power series, respectively, over $\mathbb{F}_q$. Christol [4] (see also [5]) proved that an element $x = \sum_{i=0}^{\infty} x_i t^i$ of $\mathbb{F}_q((t))$ is algebraic over

Manuscrit reçu le 20 novembre 2004.

$\mathbb{F}_q(t)$ (that is, is the root of a monic polynomial in one variable with coefficients in $\mathbb{F}_q(t)$) if and only if for each $c \in \mathbb{F}_q$, the set of base p expansions of the integers i for which $x_i = c$ is generated by a finite automaton.

However, this is not the end of the story, for there are monic polynomials over $\mathbb{F}_q(t)$ which do not have any roots in $\mathbb{F}_q((t))$, even if you enlarge the finite field and/or replace t by a root. An example, due to Chevalley [3], is the polynomial

$$x^p - x - t^{-1}.$$

Note that this is a phenomenon restricted to positive characteristic (and caused by wild ramification): an old theorem of Puiseux [18, Proposition II.8] implies that if K is a field of characteristic 0, then any monic polynomial of degree n over $K(t)$ factors into linear polynomials over $L((t^{1/n}))$ for some finite extension field L of K and some positive integer n.

1.2. Beyond Christol's theorem: generalized power series. As suggested by Abhyankar [1], the situation described in the previous section can be remedied by allowing certain "generalized power series"; these were in fact first introduced by Hahn [8] in 1907. We will define these more precisely in Section 3.1; for now, think of a generalized power series as a series $\sum_{i \in I} x_i t^i$ where the index set I is a well-ordered subset of the rationals (i.e., a subset containing no infinite decreasing sequence). For example, in the ring of generalized power series over $\mathbb{F}_p$, Chevalley's polynomial has the roots

$$x = c + t^{-1/p} + t^{-1/p^2} + \cdots$$

for $c = 0, 1, \ldots, p-1$.

Denote the field of generalized power series over $\mathbb{F}_q$ by $\mathbb{F}_q((t^{\mathbb{Q}}))$. Then it turns out that $\mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraically closed, and one can explicitly characterize those of its elements which are the roots of polynomials over $\mathbb{F}_q((t))$ [11]. One then may ask whether one can, in the vein of Christol, give an automata-theoretic characterization of the elements of $\mathbb{F}_q((t^{\mathbb{Q}}))$ which are roots of monic polynomials over $\mathbb{F}_q(t)$.

In this paper, we give such an automata-theoretic characterization. (The characterization appeared previously in the unpublished preprint [13]; this paper is an updated and expanded version of that one.) In the process, we characterize well-ordered sets of nonnegative rational numbers with terminating base b expansions ($b > 1$ an integer) which are generated by a finite automaton, and describe some techniques that may be useful for computing in the algebraic closure of $\mathbb{F}_q(t)$, such as an analogue of Newton's algorithm. (One thing we do not do is give an independent derivation of Christol's theorem; the new results here are essentially orthogonal to that result.) Whether one can use automata in practice to perform some sort of "interval arithmetic" is an intriguing question about which we will not say anything conclusive, though we do make a few speculative comments in Section 8.1.

1.3. Structure of the paper. To conclude this introduction, we describe the contents of the remaining chapters of the paper.

In Chapter 2, we collect some relevant background material on deterministic finite automata (Section 2.1), nondeterministic finite automata (Section 2.2), and the relationship between automata and base b expansions of rational numbers (Section 2.3).

In Chapter 3, we collect some relevant background material on generalized power series (Section 3.1), algebraic elements of field extensions (Section 3.2), and additive polynomials (Section 3.3).

In Chapter 4, we state our main theorem relating generalized power series algebraic over $\mathbb{F}_q(t)$ with automata, to be proved later in the paper. We formulate the theorem and note some corollaries (Section 4.1), then refine the statement by checking its compatibility with decimation of a power series (Section 4.2).

In Chapter 5, we give one complete proof of the main theorem, which in one direction relies on a certain amount of sophisticated algebraic machinery. We give a fairly direct proof that automatic generalized power series are algebraic (Section 5.1), then give a proof of the reverse implication by specializing the results of [11] (Section 5.2); the dependence on [11] is the source of the reliance on algebraic tools, such as Artin-Schreier theory.

In Chapter 6, we collect more results about fields with a valuation, specifically in the case of positive characteristic. We recall basic properties of twisted polynomials (Section 6.1) and Newton polygons (Section 6.2), give a basic form of Hensel's lemma on splitting polynomials (Section 6.3), and adapt this result to twisted polynomials (Section 6.4).

In Chapter 7, we give a second proof of the reverse implication of the main theorem, replacing the algebraic methods of the previous chapter with more explicit considerations of automata. To do this, we analyze the transition graphs of automata which give rise to generalized power series (Section 7.1), show that the class of automatic generalized power series is closed under addition and multiplication (Section 7.2), and exhibit a positive-characteristic analogue of Newton's iteration (Section 7.3).

In Chapter 8, we raise some further questions about the algorithmics of automatic generalized power series (Section 8.1), and about a potential generalization of the multivariate analogue of Christol's theorem (Section 8.2).

Acknowledgments. Thanks to Bjorn Poonen for bringing the work of Christol to the author's attention, to Eric Rains for some intriguing suggestions concerning efficient representations, to Richard Stanley for pointing out the term "cactus", and to George Bergman for helpful discussions. The author was supported previously by an NSF Postdoctoral Fellowship and currently by NSF grant DMS-0400727.

2. Automata

In this chapter, we recall notions and fix notation and terminology regarding finite automata. We take as our reference [2, Chapter 4]. We note in passing that a sufficiently diligent reader should be able to reproduce the proofs of all cited results in this chapter.

2.1. Deterministic automata.

Definition 2.1.1. A *deterministic finite automaton*, or *DFA* for short, is a tuple $M = (Q, \Sigma, \delta, q_0, F)$, where

- Q is a finite set (the *states*);
- Σ is another set (the *input alphabet*);
- δ is a function from $Q \times \Sigma$ to Q (the *transition function*);
- $q_0 \in Q$ is a state (the *initial state*);
- F is a subset of Q (the *accepting states*).

Definition 2.1.2. Let Σ^* denote the set of finite sequences consisting of elements of Σ; we will refer to elements of Σ as *characters* and elements of Σ^* as *strings*. We identify elements of Σ with one-element strings, and denote concatenation of strings by juxtaposition: that is, if s and t are strings, then st is the string composed of the elements of s followed by the elements of t. We define a *language* (over Σ) to be any subset of Σ^*.

It is sometimes convenient to represent a DFA using a transition graph.

Definition 2.1.3. Given a DFA $M = (Q, \Sigma, \delta, q_0, F)$, the *transition graph* of M is the edge-labeled directed graph (possibly with loops) on the vertex set Q, with an edge from $q \in Q$ to $q' \in Q$ labeled by $s \in \Sigma$ if $\delta(q, s) = q'$. The transition graph also comes equipped with a distinguished vertex corresponding to q_0, and a distinguished subset of the vertex set corresponding to F; from these data, one can recover M from its transition graph.

One can also imagine a DFA as a machine with a keyboard containing the elements of Σ, which can be at any time in any of the states. When one presses a key, the machine transitions to a new state by applying δ to the current state and the key pressed. One can then extend the transition function to strings by pressing the corresponding keys in sequence. Formally, we extend δ to a function $\delta^* : Q \times \Sigma^* \to Q$ by the rules

$$\delta^*(q, \emptyset) = q, \quad \delta^*(q, xa) = \delta(\delta^*(q, x), a) \qquad (q \in Q, x \in \Sigma^*, a \in \Sigma).$$

Definition 2.1.4. We say that M *accepts* a string $x \in \Sigma^*$ if $\delta^*(q_0, x) \in F$, and otherwise say it *rejects* x. The set of strings accepted by M is called the *language accepted by* M and denoted $L(M)$. A language is said to be *regular* if it is accepted by some DFA.

Lemma 2.1.5. (a) *The collection of regular languages is closed under complement, finite union, and finite intersection. Also, any language consisting of a single string is regular.*
(b) *The collection of regular languages is closed under reversal (the operation on strings taking* $s_1 \cdots s_n$ *to* $s_n \cdots s_1$*).*
(c) *A language is regular if and only if it is generated by some regular expression (see* [2, 1.3] *for a definition).*

Proof. (a) is straightforward, (b) is [2, Corollary 4.3.5], and (c) is Kleene's theorem [2, Theorem 4.1.5]. □

The Myhill-Nerode theorem [2, Theorem 4.1.8] gives an intrinsic characterization of regular languages, without reference to an auxiliary automaton.

Definition 2.1.6. Given a language L over Σ, define the equivalence relation $\sim_L$ on Σ^* as follows: $x \sim_L y$ if and only if for all $z \in \Sigma^*$, $xz \in L$ if and only if $yz \in L$.

Lemma 2.1.7 (Myhill-Nerode theorem)**.** *The language* L *is regular if and only if* Σ^* *has only finitely many equivalence classes under* $\sim_L$.

Moreover, if L is regular, then the DFA in which:

- Q is the set of equivalence classes under $\sim_L$;
- δ, applied to the class of some $x \in \Sigma^*$ and some $s \in \Sigma$, returns the class of xs;
- q_0 is the class of the empty string;
- F is the set of classes of elements of L;

generates L and has fewer states than any nonisomorphic DFA which also generates L [2, Corollary 4.1.9].

It will also be convenient to permit automata to make non-binary decisions about strings.

Definition 2.1.8. A *deterministic finite automaton with output*, or *DFAO* for short, is a tuple $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$, where

- Q is a finite set (the *states*);
- Σ is another set (the *input alphabet*);
- δ is a function from $Q \times \Sigma$ to Q (the *transition function*);
- $q_0 \in Q$ is a state (the *initial state*);
- Δ is a finite set (the *output alphabet*);
- τ is a function from Q to Δ (the *output function*).

A DFAO M gives rise to a function $f_M : \Sigma^* \to \Delta$ by setting $f_M(w) = \tau(\delta^*(q_0, w))$. Any function $f : \Sigma^* \to \Delta$ equal to f_M for some DFAO M is called a *finite-state function*; note that f is a finite-state function if and only if $f^{-1}(d)$ is a regular language for each $d \in \Delta$ [2, Theorems 4.3.1 and 4.3.2].

We will identify each DFA with the DFAO with output alphabet $\{0,1\}$ which outputs 1 on a string if the original DFA accepts the string and 0 otherwise.

It will also be useful to have devices that can operate on the class of regular languages.

Definition 2.1.9. A *finite-state transducer* is a tuple $T = (Q, \Sigma, \delta, q_0, \Delta, \lambda)$, where

- Q is a finite set (the *states*);
- Σ is another set (the *input alphabet*);
- δ is a function from $Q \times \Sigma$ to Q (the *transition function*);
- $q_0 \in Q$ is a state (the *initial state*);
- Δ is a finite set (the *output alphabet*);
- λ is a function from $Q \times \Sigma$ to Δ^* (the *output function*).

If the output of λ is always a string of length k, we say the transducer T is *k-uniform*.

A transducer T gives rise to a function $f_T : \Sigma^* \to \Delta^*$ as follows: given a string $w = s_1 \cdots s_r \in \Sigma^*$ (with each $s_i \in \Sigma$), put $q_i = \delta^*(s_1 \cdots s_i)$ for $i = 1, \dots, r$, and define

$$f_T(w) = \lambda(q_0, s_1)\lambda(q_1, s_2) \cdots \lambda(q_{r-1}, s_r).$$

That is, feed w into the transducer and at each step, use the current state and the next transition to produce a piece of output, then string together the outputs. For $L \subseteq \Sigma^*$ and $L' \subseteq \Delta^*$ languages, we write

$$f_T(L) = \{f_T(w) : w \in L\}$$
$$f_T^{-1}(L') = \{w \in \Sigma^* : f_T(w) \in L'\}.$$

Then one has the following result [2, Theorems 4.3.6 and 4.3.8].

Lemma 2.1.10. *Let T be a finite-state transducer. If $L \subseteq \Sigma^*$ is a regular language, then $f_T(L)$ is also regular; if $L' \subseteq \Delta^*$ is a regular language, then $f_T^{-1}(L')$ is also regular.*

2.2. Nondeterministic automata and multiplicities. Although they do not expand the boundaries of the theory, it will be useful in practice to allow so-called “nondeterministic automata”.

Definition 2.2.1. A *nondeterministic finite automaton*, or *NFA* for short, is a tuple $M = (Q, \Sigma, \delta, q_0, F)$, where

- Q is a finite set (the *states*);

- Σ is another set (the *input alphabet*);
- δ is a function from $Q \times \Sigma$ to the power set of Q (the *transition function*);
- $q_0 \in Q$ is a state (the *initial state*);
- F is a subset of Q (the *accepting states*).

For M an NFA and $w = s_1 \dots s_n \in \Sigma^*$ (with $s_i \in \Sigma$ for $i = 1, \dots, n$), define an *accepting path* for w to be a sequence of states $q_1, \dots, q_n \in Q$ such that $q_i \in \delta(q_{i-1}, s_i)$ for $i = 1, \dots, n$ and $q_n \in F$. Define the *language accepted by M* as the set of strings $w \in \Sigma^*$ for which there exists an accepting path.

Informally, an NFA is a machine which may make a choice of how to transition based on the current state and key pressed, or may not be able to make any transition at all. It accepts a string if there is some way it can transition from the initial state into an accepting state via the corresponding key presses.

Every DFA can be viewed as an NFA, and the language accepted is the same under both interpretations; hence every language accepted by some DFA is also accepted by some NFA. The converse is also true [2, Theorem 4.1.3], so for theoretical purposes, it is typically sufficient to work with the conceptually simpler DFAs. However, the conversion from an NFA of n states may produce a DFA with as many as 2^n states, so in practice this is not usually a good idea.

We will need the following quantitative variant of [2, Theorem 4.1.3].

Lemma 2.2.2. *Fix a positive integer n. Let $M = (Q, \Sigma, \delta, q_0, F)$ be an NFA, and let $f : \Sigma^* \to \mathbb{Z}/n\mathbb{Z}$ be the function that assigns to $w \in \Sigma^*$ the number of accepting paths for w in M, reduced modulo n. Then f is a finite-state function.*

Proof. We construct a DFAO $M' = (Q', \Sigma', \delta', q_0', \Delta', \tau')$ with the property that $f = f_{M'}$, as follows. Let Q' denote the set of functions from Q to $\mathbb{Z}/n\mathbb{Z}$, and put $\Sigma' = \Sigma$. Define the function $\delta' : Q' \times \Sigma \to Q'$ as follows: given a function $g : Q \to \mathbb{Z}/n\mathbb{Z}$ and an element $s \in \Sigma$, let $\delta'(g, s) : Q \to \mathbb{Z}/n\mathbb{Z}$ be the function given by

$$\delta'(g,s)(q) = \sum_{q_1 \in Q : \delta(q_1, s) = q} g(q_1).$$

Let $q_0' : Q \to \mathbb{Z}/n\mathbb{Z}$ be the function carrying q_0 to 1 and all other states to 0. Put $\Delta' = \mathbb{Z}/n\mathbb{Z}$, and let $\tau' : Q' \to \mathbb{Z}/n\mathbb{Z}$ be the function given by

$$\tau'(g) = \sum_{q \in F} g(q).$$

Then M' has the desired properties. □

Note that lemma 2.2.2 still works if we allow the values of δ to be multisets.

2.3. Base expansions and automatic functions. In this section, we make precise the notion of "a function on $\mathbb{Q}$ computable by a finite automaton", and ultimately relate it to the notion of an "automatic sequence" from [2, Chapter 5]. To do this, we need to fix a way to input rational numbers into an automaton, by choosing some conventions about base expansions.

Let $b > 1$ be a fixed positive integer. All automata in this section will have input alphabet $\Sigma = \Sigma_b = \{0, 1, \dots, b-1, .\}$, which we identify with the base b digits and radix point.

Definition 2.3.1. A string $s = s_1 \dots s_n \in \Sigma^*$ is said to be a *valid base b expansion* if $s_1 \neq 0$, $s_n \neq 0$, and exactly one of $s_1, \dots, s_n$ is equal to the radix point. If s is a valid base b expansion and s_k is the radix point, then we define the *value* of s to be

$$v(s) = \sum_{i=1}^{k-1} s_i b^{k-1-i} + \sum_{i=k+1}^{n} s_i b^{k-i}.$$

It is clear that no two valid strings have the same value; we may thus unambiguously define s to be the *base b expansion of* $v(s)$. Let S_b be the set of nonnegative b-adic rationals, i.e., numbers of the form m/b^n for some nonnegative integers m, n; it is also clear that the set of values of valid base b expansions is precisely S_b. For $v \in S_b$, write $s(v)$ for the base b expansion of v.

Lemma 2.3.2. *The set of valid base b expansions is a regular language.*

Proof. The language L_1 of strings with no leading zero is regular by virtue of Lemma 2.1.7: the equivalence classes under $\sim_{L_1}$ consist of the empty string, all nonempty strings in L_1, and all nonempty strings not in L_1. The language L_2 of strings with no trailing zero is also regular: the equivalence classes under $\sim_{L_2}$ consist of all strings in L_2, and all strings not in L_2. (One could also apply Lemma 2.1.5(b) to L_1 to show that L_2 is regular, or vice versa.) The language L_3 of strings with exactly one radix point is also regular: the equivalence classes under $\sim_{L_3}$ consist of all strings with zero points, all strings with one point, and all strings with more than one point. Hence $L_1 \cap L_2 \cap L_3$ is regular by Lemma 2.1.5(a), as desired. $\square$

The "real world" convention for base b expansions is a bit more complicated than what we are using: normally, one omits the radix point when there are no digits after it, one adds a leading zero in front of the radix point when there are no digits before it, and one represents 0 with a single zero rather than a bare radix point (or the empty string). This will not change anything essential, thanks to the following lemma.

Lemma 2.3.3. *Let S be a set of nonnegative b-adic rationals. Then the set of expansions of S, under our convention, is a regular language if and only if the set of "real world" expansions of S is a regular language.*

Proof. We may as well assume for simplicity that $0 \notin S$ since any singleton language is regular. Put

$$S_1 = S \cap (0,1), \qquad S_2 = S \cap \mathbb{Z}, \qquad S_3 = S \setminus (S_1 \cup S_2).$$

Then the expansions of S, under either convention, form a regular language if and only if the same is true of S_1, S_2, S_3. Namely, under our convention, the language of strings with no digits before the radix point and the language of strings with no digits after the radix point are regular. Under the "real world" convention, the language of strings with no radix point and the language of strings with a single 0 before the radix point are regular.

The expansions of S_3 are the same in both cases, so we can ignore them. For S_1, note that the language of its real world expansions is regular if and only if the language of the reverses of those strings is regular (Lemma 2.1.5(b)), if and only if the language of those reverses with a radix point added in front is regular (clear), if and only if the language of the reverses of those (which are the expansions under our convention) is regular. For S_2, note that the language of real world expansions is regular if and only if the language of those strings with the initial zeroes removed is regular. □

Definition 2.3.4. Let M be a DFAO with input alphabet Σ_b. We say a state $q \in Q$ is *preradix* (resp. *postradix*) if there exists a valid base b expansion $s = s_1 \cdots s_n$ with s_k equal to the radix point such that, if we set $q_i = \delta(q_{i-1}, s_i)$, then $q = q_i$ for some $i < k$ (resp. for some $i \geq k$). That is, when tracing through the transitions produced by s, q appears before (resp. after) the transition producing the radix point. Note that if the language accepted by M consists only of valid base b expansions, then no state can be both preradix and postradix, or else M would accept some string containing more than one radix point.

Definition 2.3.5. Let Δ be a finite set. A function $f : S_b \to \Delta$ is *b-automatic* if there is a DFAO M with input alphabet Σ and output alphabet Δ such that for any $v \in S_b$, $f(v) = f_M(s(v))$. By Lemma 2.3.2, it is equivalent to require that for some symbol $\star \notin \Delta$, there is a DFAO M with input alphabet Σ and output alphabet $\Delta \cup \{\star\}$ such that

$$f_M(s) = \begin{cases} f(v(s)) & s \text{ is a valid base } b \text{ expansion} \\ \star & \text{otherwise.} \end{cases}$$

We say a subset S of S_b is *b-regular* if its characteristic function

$$\chi_S(s) = \begin{cases} 1 & s \in S \\ 0 & s \notin S \end{cases}$$

is b-automatic; then a function $f : S_b \to \Delta$ is b-automatic if and only if $f^{-1}(d)$ is b-regular for each $d \in \Delta$.

Lemma 2.3.6. *Let $S \subseteq S_b$ be a subset. Then for any $r \in \mathbb{N}$ and any $s \in S_b$, S is b-regular if and only if*

$$rS + s = \{rx + s : x \in S\}$$

is b-regular.

Proof. As in [2, Lemmas 4.3.9 and 4.3.11], one can construct a finite-state transducer that performs the operation $x \mapsto rx + s$ on valid base b expansions read from right to left, by simply transcribing the usual hand calculation. (Remember that reversing the strings of a language preserves regularity by Lemma 2.1.5, so there is no harm in reading base b expansions backwards.) Lemma 2.1.10 then yields the desired result. □

We conclude this section by noting the relationship with the notion of "automatic sequences" from [2, Chapter 5]. In [2, Definition 5.1.1], a sequence $\{a_l\}_{l=0}^{\infty}$ over Δ is said to be *b-automatic* if there is a DFAO M with input alphabet $\{0, \dots, b-1\}$ and output alphabet Δ such that for any string $s = s_1 \cdots s_n$, if we put $v(s) = \sum_{i=1}^{n} s_i b^{n-1-i}$, then $a_{v(s)} = f_M(s)$. Note that this means M must evaluate correctly even on strings with leading zeroes, but by [2, Theorem 5.2.1], it is equivalent to require that there exists such an M only having the property that $a_{v(s)} = f_M(s)$ when $s_1 \neq 0$. It follows readily that $\{a_l\}_{l=0}^{\infty}$ is b-automatic if and only if for some symbol $\star \notin \Delta$, the function $f : S_b \to \Delta \cup \{\star\}$ defined by

$$f(x) = \begin{cases} a_x & x \in \mathbb{Z} \\ \star & \text{otherwise} \end{cases}$$

is b-automatic.

3. Algebraic preliminaries

In this chapter, we recall the algebraic machinery that will go into the formulation of Theorem 4.1.3.

3.1. Generalized power series. Let R be an arbitrary ring. Then the ring of ordinary power series over R can be identified with the ring of functions from $\mathbb{Z}_{\geq 0}$ to R, with addition given termwise and multiplication given by convolution

$$(fg)(k) = \sum_{i+j=k} f(i)g(j);$$

the latter makes sense because for any fixed $k \in \mathbb{Z}_{\geq 0}$, there are only finitely many pairs $(i, j) \in \mathbb{Z}_{\geq 0}^2$ such that $i + j = k$. In order to generalize this construction to index sets other than $\mathbb{Z}_{\geq 0}$, we will have to restrict the nonzero values of the functions so that computing fg involves adding only finitely many nonzero elements of R. The recipe for doing this dates back to Hahn [8] (although the term "Mal'cev-Neumann series" for an object of the type we describe is prevalent), and we recall it now; see also [15, Chapter 13].

Definition 3.1.1. Let G be a totally ordered abelian group (written additively) with identity element 0; that is, G is an abelian group equipped with a binary relation $>$ such that for all $a, b, c \in G$,

$$a \not> a$$
$$a \not> b, b \not> a \Rightarrow a = b$$
$$a > b, b > c \Rightarrow a > c$$
$$a > b \Leftrightarrow a + c > b + c.$$

Let P be the set of $a \in G$ for which $a > 0$; P is called the *positive cone* of G.

Lemma 3.1.2. *Let S be a subset of G. Then the following two conditions are equivalent.*

(a) *Every nonempty subset of S has a minimal element.*
(b) *There is no infinite decreasing sequence $s_1 > s_2 > \cdots$ within S.*

Proof. If (a) holds but (b) did not, then the set $\{s_1, s_2, \dots\}$ would not have a minimal element, a contradiction. Hence (a) implies (b). Conversely, if T were a subset of S with no smallest element, then for any $s_i \in T$, we could choose $s_{i+1} \in T$ with $s_i > s_{i+1}$, thus forming an infinite decreasing sequence. Hence (b) implies (a). □

Definition 3.1.3. A subset S of G is *well-ordered* if it satisfies either of the equivalent conditions of Lemma 3.1.2. (Those who prefer to avoid assuming the axiom of choice should take (a) to be the definition, as the implication (b) $\Longrightarrow$ (a) requires choice.)

For $S_1, \dots, S_n \subseteq G$, write $S_1 + \cdots + S_n$ for the set of elements of G of the form $s_1 + \cdots + s_n$ for $s_i \in S_i$; in case $S_1 = \cdots = S_n$, we abbreviate this notation to S^{+n}. (In [15] the notation nS is used instead, but we have already defined this as the dilation of S by the factor n.) Then one can easily verify the following (or see [15, Lemmas 13.2.9 and 13.2.10]).

Lemma 3.1.4. (i) *If $S_1, \dots, S_n$ are well-ordered subsets of G, then $S_1 + \cdots + S_n$ is well-ordered.*

(ii) *If $S_1, \cdots, S_n$ are well-ordered subsets of G, then for any $x \in G$, the number of n-tuples $(s_1, \dots, s_n) \in S_1 \times \cdots \times S_n$ such that $s_1 + \cdots + s_n = x$ is finite.*

(iii) *If S is a well-ordered subset of P, then $\tilde{S} = \cup_{n=1}^{\infty} S^{+n}$ also is well-ordered; moreover, $\cap_{n=1}^{\infty} \tilde{S}^{+n} = \emptyset$.*

Definition 3.1.5. Given a function $f : G \to R$, the *support* of f is the set of $g \in G$ such that $f(g) \neq 0$. A *generalized Laurent series* over R with exponents in G is a function $f : G \to R$ whose support is well-ordered; if the support is contained in $P \cup \{0\}$, we call f a *generalized power series.* We typically represent the generalized Laurent series f in series notation $\sum_i f(i)t^i$, and write $R[\![t^G]\!]$ and $R((t^G))$ for the sets of generalized power series and generalized Laurent series, respectively, over R with exponents in G.

Thanks to Lemma 3.1.4, the termwise sum and convolution product are well-defined binary operations on $R[\![t^G]\!]$ and $R((t^G))$, which form rings under the operations. A nonzero element of $R((t^G))$ is a unit if and only if its first nonzero coefficient is a unit [15, Theorem 13.2.11]; in particular, if R is a field, then so is $R((t^G))$.

3.2. Algebraic elements of fields. In this section, we recall the definition of algebraicity of an element of one field over a subfield, and then review some criteria for algebraicity. Nothing in this section is even remotely original, as can be confirmed by any sufficiently detailed abstract algebra textbook.

Definition 3.2.1. Let $K \subseteq L$ be fields. Then $\alpha \in L$ is said to be *algebraic over* K if there exists a nonzero polynomial $P(x) \in K[x]$ over K such that $P(\alpha) = 0$. We say L is *algebraic over* K if every element of L is algebraic over K.

Lemma 3.2.2. *Let $K \subseteq L$ be fields. Then $\alpha \in L$ is algebraic if and only if α is contained in a subring of L containing K which is finite dimensional as a K-vector space.*

Proof. We may as well assume $\alpha \neq 0$, as otherwise both assertions are clear. If α is contained in a subring R of L which has finite dimension m as a K-vector space, then $1, \alpha, \dots, \alpha^m$ must be linearly dependent over K, yielding a polynomial over K with α as a root. Conversely, if $P(\alpha) = 0$ for some polynomial $P(x) \in K[x]$, we may take $P(x) = c_0 + c_1 x + \cdots + c_n x^n$ with $c_0, c_n \neq 0$. In that case,

$$\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, \dots, a_{n-1} \in K\}$$

is a subring of L containing K and α, of dimension at most n as a vector space over K. □

Corollary 3.2.3. *Let $K \subseteq L$ be fields. If $\dim_K L < \infty$, then L is algebraic over K.*

Lemma 3.2.4. *Let $K \subseteq L \subseteq M$ be fields, with L algebraic over K. For any $\alpha \in M$, α is algebraic over K if and only if it is algebraic over L.*

Proof. Clearly if α is the root of a polynomial with coefficients in K, that same polynomial has coefficients in L. Conversely, suppose α is algebraic over L; it is then contained in a subring R of M which is finite dimensional over L. That subring is generated over L by finitely many elements, each of which is algebraic over K and hence lies in a subring R_i of M which is finite dimensional over K. Taking the ring generated by the R_i gives a subring of M which is finite dimensional over K and which contains α. Hence α is algebraic over K. □

Lemma 3.2.5. *Let $K \subseteq L$ be fields. If $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha + \beta$ and $\alpha\beta$. If $\alpha \neq 0$, then moreover $1/\alpha$ is algebraic over K.*

Proof. Suppose that $\alpha, \beta \in L$ are algebraic over K; we may assume $\alpha, \beta \neq 0$, else everything is clear. Choose polynomials $P(x) = c_0 + c_1 x + \cdots + c_m x^m$ and $Q(x) = d_0 + d_1 x + \cdots + d_n x^n$ with $c_0, c_m, d_0, d_n \neq 0$ such that $P(\alpha) = Q(\beta) = 0$. Then

$$R = \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij} \alpha^i \beta^j : a_{ij} \in K \right\}$$

is a subring of L containing K, of dimension at most mn as a vector space over K, containing $\alpha + \beta$ and $\alpha\beta$. Hence both of those are algebraic over K. Moreover, $1/\alpha = -(c_1 + c_2\alpha + \cdots + c_m \alpha^{m-1})/c_0$ is contained in R, so it too is algebraic over K. □

Definition 3.2.6. A field K is *algebraically closed* if every polynomial over K has a root, or equivalently, if every polynomial over K splits completely (factors into linear polynomials). It can be shown (using Zorn's lemma) that every field K is contained in an algebraically closed field; the elements of such a field which are algebraic over K form a field L which is both algebraically closed and algebraic over K. Such a field is called an *algebraic closure* of K; it can be shown to be unique up to noncanonical isomorphism, but we won't need this.

In practice, we will always consider fields contained in $\mathbb{F}_q((t^{\mathbb{Q}}))$, and constructing algebraically closed fields containing them is straightforward. That is because if K is an algebraically closed field and G is a divisible group (i.e., multiplication by any positive integer is a bijection on G), then the field $K((t^G))$ is algebraically closed. (The case $G = \mathbb{Q}$, which is the only case we need, is treated explicitly in [12, Proposition 1]; for the general case and much more, see [10, Theorem 5].) Moreover, it is easy (and does not require the axiom of choice) to construct an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$: order the elements of $\mathbb{F}_q$ with 0 coming first, then list the monic polynomials over $\mathbb{F}_q$ in lexicographic order and successively adjoin roots of them. Then the field $\overline{\mathbb{F}_q}((t^{\mathbb{Q}}))$ is algebraically closed and contains $\mathbb{F}_q((t^{\mathbb{Q}}))$.

3.3. Additive polynomials. In positive characteristic, it is convenient to restrict attention to a special class of polynomials, the "additive" polynomials. First, we recall a standard recipe (analogous to the construction of Vandermonde determinants) for producing such polynomials.

Lemma 3.3.1. *Let K be a field of characteristic $p > 0$. Given $r_1, \dots, r_n \in K$, the Moore determinant*

$$\begin{pmatrix} r_1 & r_2 & \cdots & r_n \\ r_1^p & r_2^p & \cdots & r_n^p \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{p^{n-1}} & r_2^{p^{n-1}} & \cdots & r_n^{p^{n-1}} \end{pmatrix}$$

vanishes if and only if $r_1, \dots, r_n$ are linearly dependent over $\mathbb{F}_p$.

Proof. Viewed as a polynomial in $r_1, \dots, r_n$ over $\mathbb{F}_p$, the Moore determinant is divisible by each of the linear forms $c_1 r_1 + \cdots + c_n r_n$ for $c_1, \dots, c_n \in \mathbb{F}_p$ not all zero. Up to scalar multiples, there are $p^{n-1} + \cdots + p + 1$ such forms, so the determinant is divisible by the product of these forms. However, the determinant visibly is a homogeneous polynomial in the r_i of degree $p^{n-1} + \cdots + p + 1$, so it must be equal to the product of the linear factors times a constant. The desired result follows. □

Definition 3.3.2. A polynomial $P(z)$ over a field K of characteristic $p > 0$ is said to be *additive* (or *linearized*) if it has the form

$$P(z) = c_0 z + c_1 z^p + \cdots + c_n z^{p^n}$$

for some $c_0, \dots, c_n \in K$.

Lemma 3.3.3. *Let $P(z)$ be a nonzero polynomial over a field K of characteristic $p > 0$, and let L be an algebraic closure of K. Then the following conditions are equivalent.*

(a) *The polynomial $P(z)$ is additive.*
(b) *The equation $P(y + z) = P(y) + P(z)$ holds as a formal identity of polynomials.*
(c) *The equation $P(y + z) = P(y) + P(z)$ holds for all $y, z \in L$.*
(d) *The roots of P in L form an $\mathbb{F}_p$-vector space under addition, all roots occur to the same multiplicity, and that multiplicity is a power of p.*

Proof. The implications (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) are clear, and (c) $\Longrightarrow$ (b) holds because the field L must be infinite. We next check that (d) $\Longrightarrow$ (a). Let $V \subset L$ be the set of roots, and let p^e be the common multiplicity. Let $Q(z)$ be the Moore determinant of $z^{p^e}, r_1^{p^e}, \cdots, r_m^{p^e}$. By Lemma 3.3.1, the roots of Q are precisely the elements of V, and each occurs with multiplicity at least p^e. However, $\deg(Q) = p^{e+m} = \deg(P)$, so the multiplicities must be exactly p^e, and P must equal Q times a scalar. Since Q is visibly additive, so is P.

It remains to check that (c) $\Longrightarrow$ (d). Given (c), note that the roots of P in L form an $\mathbb{F}_p$-vector space under addition; also, if $r \in L$ is a root of P, then $P(z+r) = P(z)$, so all roots of P have the same multiplicity. Let V be the roots of P, choose generators $r_1, \dots, r_m$ of V as an $\mathbb{F}_p$-vector space, and let $Q(z)$ be the Moore determinant of $z, r_1, \dots, r_m$. Then $P(z) = cQ(z)^n$ for some constant c, where n is the common multiplicity of the roots of P (because Q has no repeated roots, by the analysis of the previous paragraph). Suppose that n is not a prime power; then the polynomials $(y+z)^n$ and $y^n + z^n$ are not identically equal, because the binomial coefficient $\binom{n}{p^i}$, for i the largest integer such that p^i divides n, is not divisible by p. Thus there exist values of y, z in L for which $(y+z)^n \neq y^n + z^n$. Since L is algebraically closed, Q is surjective as a map from L to itself; we can thus choose $y, z \in L$ such that $(Q(y)+Q(z))^n \neq Q(y)^n + Q(z)^n$. Since Q is additive, this means that $P(y+z) \neq P(y) + P(z)$, contrary to hypothesis. We conclude that n must be a prime power. Hence (c) $\Longrightarrow$ (d), and the proof is complete. □

The following observation is sometimes known as "Ore's lemma" (as in [2, Lemma 12.2.3]).

Lemma 3.3.4. *For $K \subseteq L$ fields of characteristic $p > 0$ and $\alpha \in L$, α is algebraic over K if and only if it is a root of some additive polynomial over K.*

Proof. Clearly if α is a root of an additive polynomial over K, then α is algebraic over K. Conversely, if α is algebraic, then $\alpha, \alpha^p, \dots$ cannot all be linearly independent, so there must be a linear relation of the form $c_0\alpha + c_1\alpha^p + \cdots + c_n\alpha^{p^n} = 0$ with $c_0, \dots, c_n \in K$ not all zero. □

Our next lemma generalizes Lemma 3.3.4 to "semi-linear" systems of equations.

Lemma 3.3.5. *Let $K \subseteq L$ be fields of characteristic $p > 0$, let A, B be $n \times n$ matrices with entries in K, at least one of which is invertible, and let $\mathbf{w} \in K^n$ be any (column) vector. Suppose $\mathbf{v} \in L^n$ is a vector such that $A\mathbf{v}^\sigma + B\mathbf{v} = \mathbf{w}$, where σ denotes the p-th power Frobenius map. Then the entries of $\mathbf{v}$ are algebraic over K.*

Proof. Suppose A is invertible. Then for $i = 1, 2, \dots,$ we can write $\mathbf{v}^{\sigma^i} = U_i\mathbf{v} + \mathbf{w}_i$ for some $n \times n$ matrix U_i over K and some $\mathbf{w}_i \in K^n$. Such vectors span a vector space over K of dimension at most $n^2 + n$; for some m, we can thus find $c_0, \dots, c_m$ not all zero such that

$$c_0\mathbf{v} + c_1\mathbf{v}^\sigma + \cdots + c_m\mathbf{v}^{\sigma^m} = 0. \tag{3.3.6}$$

Apply Lemma 3.3.4 to each component in (3.3.6) to deduce that the entries of $\mathbf{v}$ are algebraic over K.

Now suppose B is invertible. There is no harm in enlarging L, so we may as well assume that L is closed under taking p-th roots, i.e., L is perfect. Then the map $\sigma : L \to L$ is a bijection. Let K' be the set of $x \in L$ for which there exists a nonnegative integer i such that $x^{\sigma^i} \in K$; then $\sigma : K' \to K'$ is also a bijection, and each element of K' is algebraic over K.

For $i = 1, 2, \dots$, we can now write $\mathbf{v}^{\sigma^{-i}} = U_i \mathbf{v} + \mathbf{w}_i$ for some $n \times n$ matrix U_i over K' and some $\mathbf{w}_i \in (K')^n$. As above, we conclude that the entries of $\mathbf{v}$ are algebraic over K'. However, any element $\alpha \in L$ algebraic over K' is algebraic over K: if $d_0 + d_1\alpha + \cdots + d_m\alpha^m = 0$ for $d_0, \dots, d_m \in K'$ not all zero, then we can choose a nonnegative integer i such that $d_0^{\sigma^i}, \dots, d_m^{\sigma^i}$ belong to K, and $d_0^{\sigma^i} + d_1^{\sigma^i}\alpha^{p^i} + \cdots + d_m^{\sigma^i}\alpha^{mp^i} = 0$. We conclude that the entries of $\mathbf{v}$ are algebraic over K, as desired. □

4. Generalized power series and automata

In this chapter, we state the main theorem (Theorem 4.1.3) and some related results; its proof (or rather proofs) will occupy much of the rest of the paper.

4.1. The main theorem: statement and preliminaries. We are now ready to state our generalization of Christol's theorem, the main theoretical result of this paper. For context, we first state a form of Christol's theorem (compare [4], [5], and also [2, Theorem 12.2.5]). Reminder: $\mathbb{F}_q(t)$ denotes the field of rational functions over $\mathbb{F}_q$, i.e., the field of fractions of the ring of polynomials $\mathbb{F}_q[t]$.

Theorem 4.1.1 (Christol). *Let q be a power of the prime p, and let $\{a_i\}_{i=0}^\infty$ be a sequence over $\mathbb{F}_q$. Then the series $\sum_{i=0}^\infty a_i t^i \in \mathbb{F}_q[\![t]\!]$ is algebraic over $\mathbb{F}_q(t)$ if and only if the sequence $\{a_i\}_{i=0}^\infty$ is p-automatic.*

We now formulate our generalization of Christol's theorem. Recall that S_p is the set of numbers of the form m/p^n, for m, n nonnegative integers.

Definition 4.1.2. Let q be a power of the prime p, and let $f : \mathbb{Q} \to \mathbb{F}_q$ be a function whose support S is well-ordered. We say the generalized Laurent series $\sum_i f(i)t^i$ is *p-quasi-automatic* if the following conditions hold.

(a) For some integers a and b with $a > 0$, the set $aS + b = \{ai + b : i \in S\}$ is contained in S_p, i.e., consists of nonnegative p-adic rationals.

(b) For some a, b for which (a) holds, the function $f_{a,b} : S_p \to \mathbb{F}_q$ given by $f_{a,b}(x) = f((x - b)/a)$ is p-automatic.

Note that by Lemma 2.3.6, if (b) holds for a single choice of a, b satisfying (a), then (b) holds also for any choice of a, b satisfying (a). In case (a) and (b) hold with $a = 1, b = 0$, we say the series is *p-automatic.*

Theorem 4.1.3. *Let q be a power of the prime p, and let $f : \mathbb{Q} \to \mathbb{F}_q$ be a function whose support is well-ordered. Then the corresponding generalized Laurent series $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if it is p-quasi-automatic.*

We will give two proofs of Theorem 4.1.3 in due course. In both cases, we use Proposition 5.1.2 to deduce the implication "automatic implies algebraic". For the reverse implication "algebraic implies automatic", we use Proposition 5.2.7 for a conceptual proof and Proposition 7.3.4 for a more algorithmic proof. Note, however, that both of the proofs in this direction rely on Christol's theorem, so we do not obtain an independent derivation of that result.

Corollary 4.1.4. *The generalized Laurent series $\sum_i f(i)t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if for each $\alpha \in \mathbb{F}_q$, the generalized Laurent series*

$$\sum_{i \in f^{-1}(\alpha)} t^i$$

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

We mention another corollary following [2, Theorem 12.2.6].

Definition 4.1.5. Given two generalized Laurent series $x = \sum_i x_i t^i$ and $y = \sum_i y_i t^i$ in $\mathbb{F}_q((t^{\mathbb{Q}}))$, then $\sum_i (x_i y_i) t^i$ is also a generalized Laurent series; it is called the *Hadamard product* and denoted $x \odot y$. Then one has the following assertion, which in the case of ordinary power series is due to Furstenberg [7].

Corollary 4.1.6. *If $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ are algebraic over $\mathbb{F}_q(t)$, then so is $x \odot y$.*

Proof. Thanks to Theorem 4.1.3, this follows from the fact that if $f : \Sigma^* \to \Delta_1$ and $g : \Sigma^* \to \Delta_2$ are finite-state functions, then so is $f \times g : \Sigma^* \to \Delta_1 \times \Delta_2$; the proof of the latter is straightforward (or compare [2, Theorem 5.4.4]). □

4.2. Decimation and algebraicity. Before we attack Theorem 4.1.3 proper, it will be helpful to know that the precise choice of a, b in Theorem 4.1.3, which does not matter on the automatic side (Definition 4.1.2), also does not matter on the algebraic side.

Definition 4.2.1. For $\tau \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, regard τ as an automorphism of $\mathbb{F}_q(t)$ and $\mathbb{F}_q((t^{\mathbb{Q}}))$ by allowing it to act on coefficients. That is,

$$\left(\sum_i x_i t^i\right)^\tau = \sum_i x_i^\tau t^i.$$

Let $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ denote the p-power Frobenius map; note that the convention we just introduced means that $x^p = x^\sigma$ if $x \in \mathbb{F}_q$, but not if $x \in \mathbb{F}_q(t)$ or $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$.

Lemma 4.2.2. *Let a, b be integers with $a > 0$. Then $\sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t)$ if and only if $\sum_i x_{ai+b} t^i$ is algebraic over $\mathbb{F}_q(t)$.*

Proof. It suffices to prove the result in the case $a = 1$ and in the case $b = 0$, as the general case follows by applying these two in succession. The case $a = 1$ is straightforward: if $x = \sum_i x_i t^i$ is a root of the polynomial $P(z)$ over $\mathbb{F}_q(t)$, then $x' = \sum_i x_{i+b} t^i = \sum_i x_i t^{i-b}$ is a root of the polynomial $P(zt^b)$, and vice versa.

As for the case $b = 0$, we can further break it down into two cases, one in which $a = p$, the other in which a is coprime to p. We treat the former case first. If $x = \sum_i x_i t^i$ is a root of the polynomial $P(z) = \sum c_j z^j$ over $\mathbb{F}_q(t)$, then $x' = \sum_i x_{pi} t^i = \sum_i x_i t^{i/p}$ is a root of the polynomial

$$\sum c_j^\sigma z^{pj}$$

over $\mathbb{F}_q(t)$. Conversely, if x' is a root of the polynomial $Q(z) = \sum d_j z^j$ over $\mathbb{F}_q(t)$, then x is a root of the polynomial

$$\sum (d_j^p)^{\sigma^{-1}} z^j$$

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

Now suppose that $b = 0$ and a is coprime to p. Let $\tau : \mathbb{F}_q((t^{\mathbb{Q}})) \to \mathbb{F}_q((t^{\mathbb{Q}}))$ denote the automorphism $\sum x_i t^i \mapsto \sum x_i t^{ai}$; then τ also acts on $\mathbb{F}_q(t)$. If $x = \sum_i x_i t^i$ is a root of the polynomial $P(z) = \sum c_j z^j$ over $\mathbb{F}_q(t)$, then $x' = \sum_i x_{ai} t^i = \sum_i x_i t^{i/a}$ is a root of the polynomial

$$\sum c_j^{\tau^{-1}} z^j$$

over $\mathbb{F}_q(t^{1/a})$; since $\mathbb{F}_q(t^{1/a})$ is finite dimensional over $\mathbb{F}_q(t)$, x' is algebraic over $\mathbb{F}_q(t)$ by Lemma 3.2.4. Conversely, if x' is a root of the polynomial $Q(z) = \sum d_j z^j$ over $\mathbb{F}_q(t)$, then x is a root of the polynomial

$$\sum c_j^\tau z^j$$

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

We have now proved the statement of the lemma in case $a = 1$ and b is arbitrary, in case $a = p$ and $b = 0$, and in case a is coprime to p and $b = 0$. As noted above, these three cases together imply the desired result. □

5. Proof of the main theorem: abstract approach

In this chapter, we give a proof of Theorem 4.1.3. While the proof in the "automatic implies algebraic" direction is fairly explicit, the proof in the reverse direction relies on the results of [11], and hence is fairly conceptual. We will give a more explicit approach to the reverse direction in the next chapter.

5.1. Automatic implies algebraic. In this section, we establish the "automatic implies algebraic" direction of Theorem 4.1.3. The proof is a slight modification of the usual argument used to prove the corresponding direction of Christol's theorem (as in [2, Theorem 12.2.5]). (Note that this direction of Theorem 4.1.3 will be invoked in both proofs of the reverse direction.)

Lemma 5.1.1. *Let p be a prime number, and let S be a p-regular subset of S_p. Then $\sum_{i\in S} t^i \in \mathbb{F}_p[\![t^{\mathbb{Q}}]\!]$ is algebraic over $\mathbb{F}_p(t)$.*

Proof. Let L be the language of strings of the form $s(v)$ for $v \in S$, and let M be a DFA which accepts L.

For n a nonnegative integer, let $s'(n)$ be the base p expansion of n minus the final radix point. For each preradix state $q \in Q$, let T_q be the set of nonnegative integers n such that $\delta^*(q_0, s'(n)) = q$, put $f(q) = \sum_{i\in T_q} t^i$, and let U_q be the set of pairs $(q', d) \in Q \times \{0, \dots, p-1\}$ such that $\delta(q', d) = q$. (Note that this forces q' to be preradix.) Then if $q \neq q_0$, we have

$$f(q) = \sum_{(q',d)\in U_q} t^d f(q')^p,$$

whereas if $q = q_0$, we have

$$f(q_0) = 1 + \sum_{(q',d)\in U_q} t^d f(q')^p.$$

By Lemma 3.3.5, $f(q)$ is algebraic over $\mathbb{F}_q(t)$ for each preradix state q.

For $x \in S_p \cap [0, 1)$, let $s''(x)$ be the base p expansion of x minus the initial radix point. For each postradix state $q \in Q$, let V_q be the set of $x \in S_p \cap [0, 1)$ such that $\delta^*(q, s''(x))$ is a final state, and put $g(q) = \sum_{i\in V_q} t^i$. Then if q is non-final, we have

$$g(q)^p = \sum_{d=0}^{p-1} t^d g(\delta(q, d)),$$

whereas if q is final, then

$$g(q)^p = 1 + \sum_{d=0}^{p-1} t^d g(\delta(q, d)).$$

By Lemma 3.3.5, $g(q)$ is algebraic for each postradix state q.

Finally, note that

$$\sum_{i \in S} t^i = \sum_{q,q'} f(q)g(q'),$$

the sum running over preradix q and postradix q'. This sum is algebraic over $\mathbb{F}_q(t)$ by Lemma 3.2.5, as desired. □

Proposition 5.1.2. *Let $\sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ be a p-quasi-automatic generalized Laurent series. Then $\sum_i x_i t^i$ is algebraic over $\mathbb{F}_q(t)$.*

Proof. Choose integers a, b as in Definition 4.1.2. For each $\alpha \in \mathbb{F}_q$, let S_α be the set of $j \in \mathbb{Q}$ such that $x_{(j-b)/a} = \alpha$. Then each S_α is p-regular, so Lemma 5.1.1 implies that $\sum_{j \in S_\alpha} t^j$ is algebraic over $\mathbb{F}_q(t)$. By Lemma 3.2.5,

$$\sum_i x_{ai+b} t^i = \sum_{\alpha \in \mathbb{F}_q} \alpha \left(\sum_{j \in S_\alpha} t^j \right)$$

is also algebraic over $\mathbb{F}_q(t)$; by Lemma 4.2.2, $\sum_i x_i t^i$ is also algebraic over $\mathbb{F}_q(t)$. □

5.2. Algebraic implies automatic. We next prove the "algebraic implies automatic" direction of Theorem 4.1.3. Unfortunately, the techniques originally used to prove Christol's theorem (as in [2, Chapter 12]) do not suffice to give a proof of this direction. In this section, we will get around this by using the characterization of the algebraic closure of $\mathbb{F}_q((t))$ within $\mathbb{F}_q((t^{\mathbb{Q}}))$ provided by [11]. This proof thus inherits the property of [11] of being a bit abstract, as [11] uses some Galois theory and properties of finite extensions of fields in positive characteristic (namely Artin-Schreier theory, which comes from an argument in Galois cohomology). It also requires invoking the "algebraic implies automatic" direction of Christol's theorem itself. We will give a second, more computationally explicit proof of this direction later (Proposition 7.3.4).

Definition 5.2.1. For c a nonnegative integer, let T_c be the subset of S_p given by

$$T_c = \left\{ n - b_1 p^{-1} - b_2 p^{-2} - \cdots : n \in \mathbb{Z}_{>0}, b_i \in \{0, \ldots, p-1\}, \sum b_i \le c \right\}.$$

Then [11, Theorem 15] gives a criterion for algebraicity of a generalized power series not over the rational function field $\mathbb{F}_q(t)$, but over the Laurent series field $\mathbb{F}_q((t))$. It can be stated as follows.

Proposition 5.2.2. *For $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$, x is algebraic over $\mathbb{F}_q((t))$ if and only if the following conditions hold.*

(a) *There exist integers $a, b, c \ge 0$ such that the support of $\sum_i x_{(i-b)/a} t^i$ is contained in T_c.*

(b) *For some a, b, c as in (a), there exist positive integers M and N such that every sequence $\{c_n\}_{n=0}^{\infty}$ of the form*

$$c_n = x_{(m-b-b_1p^{-1}-\cdots-b_{j-1}p^{-j+1}-p^{-n}(b_jp^{-j}+\cdots))/a}, \tag{5.2.3}$$

with j a nonnegative integer, m a positive integer, and $b_i \in \{0, \dots, p-1\}$ such that $\sum b_i \leq c$, becomes eventually periodic with period length dividing N after at most M terms.

Moreover, in this case, (b) holds for any a, b, c as in (a).

Beware that it is possible to choose a, b so that the support of $\sum x_{(i-b)/a}t^i$ is contained in S_p and yet not have (a) satisfied for any choice of c. For example, the support of $x = \sum_{i=0}^{\infty} t^{(1-p^{-i})/(p-1)}$ is contained in S_p and in $\frac{1}{p-1}T_1$, but is not contained in T_c for any c.

We first treat a special case of the "algebraic implies automatic" implication which is orthogonal to Christol's theorem.

Lemma 5.2.4. *Suppose that $x = \sum_i x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ has support in $(0,1] \cap T_c$ for some nonnegative integer c, and that x is algebraic over $\mathbb{F}_q((t))$. Then:*

(a) *x is p-automatic;*
(b) *x is algebraic over $\mathbb{F}_q(t)$;*
(c) *x lies in a finite set determined by q and c.*

Proof. Note that (b) follows from (a) by virtue of Proposition 5.1.2, so it suffices to prove (a) and (c). The criterion from Proposition 5.2.2 applies with $a = 1, b = 0$ and the given value of c, so we have that every sequence $\{c_n\}_{n=0}^{\infty}$ of the form

$$c_n = x_{1-b_1p^{-1}-\cdots-b_{j-1}p^{-j+1}-p^{-n}(b_jp^{-j}+\cdots)}, \tag{5.2.5}$$

with $b_i \in \{0, \dots, p-1\}$ such that $\sum b_i \leq c$, becomes eventually periodic with period length dividing N after at most M terms.

Define an equivalence relation on S_p as follows. Declare two elements of S_p to be equivalent if one can obtain the base b expansion of one from the base b expansion of the other by repeating the following operation: replace a consecutive string of $M + u + vN$ zeroes by a consecutive string of $M + u + wN$ zeroes, where u, v, w may be any nonnegative integers. The criterion of Proposition 5.2.2 then asserts that if $i, j \in S_p$ satisfy $i \sim j$, then $x_{1-i} = x_{1-j}$; also, the equivalence relation is clearly stable under concatenation with a fixed postscript.

Under this equivalence relation, each equivalence class has a unique shortest element, namely the one in which no nonzero digit in the base b expansion is preceded by $M + N$ zeroes. On one hand, this means that x is determined by finitely many coefficients, so (c) follows. On the other hand, by the Myhill-Nerode theorem (Lemma 2.1.7), it follows that the function $f : S_p \to \mathbb{F}_q$ given by $f(i) = x_{1-i}$ is p-automatic. (More precisely, Lemma 2.1.7 implies that the inverse image of each element of $\mathbb{F}_q$ under f is p-regular, and hence f is p-automatic.) Since there is an obvious transducer that perfoms the operation $i \mapsto 1-i$ on the valid base b expansions of elements of $S_p \cap (0,1]$ (namely, transcribe the usual hand computation), x is p-automatic, and (a) follows. □

Lemma 5.2.6. *Suppose that $x_1, \dots, x_m \in \mathbb{F}_q((t^{\mathbb{Q}}))$ all satisfy the hypothesis of Lemma 5.2.4 for the same value of c, and that $x_1, \dots, x_m$ are linearly dependent over $\mathbb{F}_q((t))$. Then $x_1, \dots, x_m$ are also linearly dependent over $\mathbb{F}_q$.*

Proof. If $x_1, \dots, x_m$ are linearly dependent over $\mathbb{F}_q((t))$, then by clearing denominators, we can find a nonzero linear relation among them of the form $c_1 x_1 + \cdots + c_m x_m = 0$, where each c_i is in $\mathbb{F}_q[\![t]\!]$. Write $c_i = \sum_{j=0}^{\infty} c_{i,j} t^j$ for $c_{i,j} \in \mathbb{F}_q$; we then have

$$0 = \sum_{j=0}^{\infty} \left(\sum_{i=1}^{m} c_{i,j} x_i \right) t^j$$

in $\mathbb{F}_q((t^{\mathbb{Q}}))$. However, the support of the quantity in parentheses is contained in $(j, j+1]$; in particular, these supports are disjoint for different j. Thus for the sum to be zero, the summand must be zero for each j; that is, $\sum_{i=1}^{m} c_{i,j} x_i = 0$ for each j. The $c_{i,j}$ cannot all be zero or else $c_1, \dots, c_m$ would have all been zero, so we obtain a nontrivial linear relation among $x_1, \dots, x_m$ over $\mathbb{F}_q$, as desired. □

We now establish the “algebraic implies automatic” implication of Theorem 4.1.3.

Proposition 5.2.7. *Let $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ be a generalized power series which is algebraic over $\mathbb{F}_q(t)$. Then x is p-quasi-automatic.*

Proof. Choose a, b, c as in Proposition 5.2.2, and put $y_i = x_{(i-b)/a}$ and $y = \sum_i y_i t^i$, so that y is algebraic over $\mathbb{F}_q(t)$ (by Lemma 4.2.2) and has support in T_c. Note that for any positive integer m, y^{q^m} is also algebraic over $\mathbb{F}_q(t)$ and also has support in T_c. By Lemma 3.3.4, we can find a polynomial $P(z) = \sum_{i=0}^{m} c_i z^{q^i}$ over $\mathbb{F}_q(t)$ such that $P(y - y_0) = 0$. We may assume without loss of generality that $c_m \neq 0$, and that $c_l = 1$, where l is the smallest nonnegative integer for which $c_l \neq 0$.

Let V be the set of elements of $\mathbb{F}_q((t^{\mathbb{Q}}))$ which satisfy the hypotheses of Lemma 5.2.4; then V is a finite set which is a vector space over $\mathbb{F}_q$, each of whose elements is p-automatic and also algebraic over $\mathbb{F}_q(t)$. Let $v_1, \dots, v_r$ be a basis of V over $\mathbb{F}_q$; by Lemma 5.2.6, $v_1, \dots, v_r$ are also linearly independent over $\mathbb{F}_q((t))$.

By the criterion of Proposition 5.2.2, we can write $y - y_0 = \sum_{j=0}^{\infty} v_j t^j$ with each $v_j \in V$. In other words, y is an $\mathbb{F}_q((t))$-linear combination of elements of V. Likewise, for each positive integer m, $(y-y_0)^{q^m}$ is an $\mathbb{F}_q((t))$-linear combination of elements of V. For $i = l, \ldots, m$, write $(y - y_0)^{q^i} = \sum_{j=1}^{r} a_{i,j} v_j$ with $a_{i,j} \in \mathbb{F}_q((t))$; then the $a_{i,j}$ are uniquely determined by Lemma 5.2.6.

By the same reasoning, for $j = 1, \ldots, r$, we can write

$$v_h^q = \sum_{h=1}^{r} b_{h,j} v_j$$

for some $b_{h,j} \in \mathbb{F}_q[t]$. This means that

$$a_{i,j} = \sum_{h} b_{h,j} a_{i-1,h}^q \qquad (i = l+1, \ldots, m; j = 1, \ldots, r). \tag{5.2.8}$$

Moreover, the equation

$$(y - y_0)^{q^l} = -c_{l+1}((y - y_0)^{q^l})^q - \cdots - c_m((y - y_0)^{q^{m-1}})^q,$$

which holds because $P(y - y_0) = 0$ and $c_l = 1$ by hypothesis, can be rewritten as

$$\begin{aligned} \sum_{j=1}^{r} a_{l,j} v_j &= \sum_{i=l}^{m-1} -c_{i+1} (\sum_{h=1}^{r} a_{i,h} v_h)^q \\ &= \sum_{i=l}^{m-1} -c_{i+1} \sum_{h=1}^{r} \sum_{j=1}^{r} a_{i,h}^q b_{h,j} v_j. \end{aligned}$$

Equating coefficients of v_j yields a system of equations of the form

$$a_{l,j} = \sum_{g=l}^{m-1} \sum_{h=1}^{r} d_{g,h} a_{g,h}^q \tag{5.2.9}$$

with each $d_{g,h} \in \mathbb{F}_q(t)$.

Combining (5.2.8) and (5.2.9) yields a system of equations which translates into a matrix equation of the form described by Lemma 3.3.5, in which the matrix B described therein is the identity. By Lemma 3.3.5, the $a_{i,j}$ are algebraic over $\mathbb{F}_q(t)$ for $i = l, \ldots, m$.

Since each $a_{i,j}$ belongs to $\mathbb{F}_q((t))$, Christol's theorem (Theorem 4.1.1) implies that $a_{i,j}$ is p-automatic for $i = l, \ldots, m-1$ and $j = 1, \ldots, r$. This implies that $(y - y_0)^{q^l} = \sum_{j=1}^{r} a_{l,j} v_j$ is p-automatic, as follows. Write $(y - y_0)^{q^l} = \sum_{k=0}^{\infty} w_k t^k$ with $w_k \in V$. Then the function $k \mapsto w_k$ is p-automatic because the $a_{i,j}$ are p-automatic. So we can build an automaton that, given a base b expansion, sorts the preradix string k according to the value of w_k, then handles the postradix string by imitating some automaton that computes w_k.

Since $(y - y_0)^{q^l}$ is p-automatic, $y - y_0$ is p-quasi-automatic, as then is y, as then is x. This yields the desired result. □

Note that Propositions 5.1.2 and 5.2.7 together give a complete proof of Theorem 4.1.3. We will give a second proof of a statement equivalent to Proposition 5.2.7 later (see Proposition 7.3.4).

6. Polynomials over valued fields

In this chapter, we introduce some additional algebraic tools that will help us give a more algorithmic proof of the "algebraic implies automatic" implication of Theorem 4.1.3. Nothing in this chapter is particularly novel, but the material may not be familiar to nonspecialists, so we give a detailed presentation.

6.1. Twisted polynomial rings.

Ore's lemma (Lemma 3.3.4) asserts that every algebraic element of a field of characteristic p over a subfield is a root of an additive polynomial. It is sometimes more convenient to view additive polynomials as the result of applying "twisted polynomials" in the Frobenius operator. These polynomials arise naturally in the theory of Drinfeld modules; see for instance [9].

Throughout this section, the field K will have characteristic $p > 0$.

Definition 6.1.1. Let $K\{F\}$ denote the noncommutative ring whose elements are finite formal sums $\sum_{i=0}^m c_i F^i$, added componentwise and multiplied by the rule

$$\left(\sum_{i=0}^{m} c_i F^i\right)\left(\sum_{j=0}^{n} d_j F^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} c_i d_j^{p^i}\right) F^k.$$

The ring $K\{F\}$ is called the *twisted polynomial ring* over K. (Note that the same definition can be made replacing the p-power endomorphism by any endomorphism of K, but we will only use this particular form of the construction.)

Definition 6.1.2. As in the polynomial case, the *degree* of a nonzero twisted polynomial $\sum c_i F^i$ is the largest i such that $c_i \neq 0$; we conventionally take the degree of the zero polynomial to be $-\infty$. The degree of the product of two nonzero twisted polynomials is the sum of their individual degrees; in particular, the ring $K\{F\}$ is an integral domain.

Twisted polynomial rings admit the following right division algorithm, just as in the usual polynomial case.

Lemma 6.1.3. *Let $S(F)$ and $T(F)$ be twisted polynomials over K, with $T(F)$ nonzero and $\deg(T) = d \geq 0$. Then there exists a unique pair $Q(F), R(F)$ of twisted polynomials over K with $\deg(R) < d$, such that $S = QT + R$.*

Proof. Write $T(F) = \sum_{i=0}^{d} c_i F^i$ with $c_d \neq 0$. Existence follows by induction on $\deg(S)$ and the fact that we can construct a left multiple of T of any prescribed degree $e \geq d$ with any prescribed leading coefficient a (namely $(a/c_d^{p^{e-d}})F^{e-d}T$). Uniqueness follows from the fact that if $S = QT + R = Q'T + R'$ are two decompositions of the desired form, then $R - R' = (Q' - Q)T$ is a left multiple of T but $\deg(R - R') < \deg(T)$, so $R - R' = 0$. □

We may view twisted polynomials over K as additive operators on any field L containing K by declaring that

$$\left(\sum_i c_i F^i\right)(z) = \sum_i c_i z^{p^i}.$$

Lemma 6.1.4. *Let L be an algebraic closure of K, and let $T(F) = \sum_{i=0}^{d} c_i F^i$ be a nonzero twisted polynomial of degree d over K. Then the kernel $\ker_L(T)$ of T acting on L is an $\mathbb{F}_p$-vector space of dimension $\leq d$, with equality if and only if $c_0 \neq 0$.*

Proof. The kernel is an $\mathbb{F}_p$-vector space because $T(F)$ is an additive operator on L (Lemma 3.3.3), and the dimension bound holds because $T(F)(z)$ is a polynomial in z of degree p^d. The equality case holds because the formal derivative in z of $T(F)(z)$ is c_0, and this derivative vanishes if and only if $T(F)(z)$ has no repeated roots over L. □

Lemma 6.1.5. *Let $S(F)$ and $T(F)$ be twisted polynomials over K, with the constant coefficient of T nonzero, and let L be an algebraic closure of K. Then S is a left multiple of T (that is, $S = QT$ for some $Q \in K\{F\}$) if and only if $\ker_L(T) \subseteq \ker_L(S)$.*

Proof. If $S = QT$, then $T(F)(z) = 0$ implies $S(F)(z) = 0$, so $\ker_L(T) \subseteq \ker_L(S)$. Conversely, suppose that $\ker_L(T) \subseteq \ker_L(S)$, and write $S = QT + R$ by the right division algorithm; we then have $\ker_L(T) \subseteq \ker_L(R)$ as well. By Lemma 6.1.4, $\ker_L(T)$ is an $\mathbb{F}_p$-vector space of dimension $\deg(T)$; if R is nonzero, then $\ker_L(R)$ is an $\mathbb{F}_p$-vector space of dimension at most $\deg(R) < \deg(T)$. But that would contradict the inclusion $\ker_L(T) \subseteq \ker_L(R)$, so we must have $R = 0$ and $S = QT$, as desired. □

6.2. Newton polygons. The theory of Newton polygons is a critical ingredient in the computational and theoretical study of valued fields. We recall a bit of this theory here.

Definition 6.2.1. For $x \in \mathbb{F}_q((t^{\mathbb{Q}}))$ nonzero, let $v(x)$ denote the smallest element of the support of x; we call v the *valuation* on $\mathbb{F}_q((t^{\mathbb{Q}}))$. We also formally put $v(0) = \infty$. The function v has the usual properties of a valuation:

$$v(x+y) \geq \min\{v(x), v(y)\}$$
$$v(xy) = v(x) + v(y).$$

Given a nonzero polynomial $P(z) = \sum_i c_i z^i$ over $\mathbb{F}_q((t^{\mathbb{Q}}))$, we define the *Newton polygon* of P to be the lower boundary of the lower convex hull of the set of points $(-i, v(c_i))$. The slopes of this polygon are called the *slopes* of P; for $r \in \mathbb{Q}$, we define the *multiplicity* of r as a slope of P to be the width (difference in x-coordinates between the endpoints) of the segment of the Newton polygon of P of slope r, or 0 if no such segment exists. We say P is *pure (of slope r)* if all of the slopes of P are equal to r. We conventionally declare that ∞ may also be a slope, and its multiplicity as a slope of a polynomial P is the order of vanishing of P at $z = 0$.

Lemma 6.2.2. *Let P and Q be nonzero polynomials over $\mathbb{F}_q((t^{\mathbb{Q}}))$. Then for each $r \in \mathbb{Q} \cup \{\infty\}$, the multiplicity of r as a slope of $P+Q$ is the sum of the multiplicities of r as a slope of P and of Q.*

Proof. The case $r = \infty$ is clear, so we assume $r \in \mathbb{Q}$. Write $P(z) = \sum_i c_i z^i$ and $Q(z) = \sum_j d_j z^j$. Let $(-e, v(c_e))$ and $(-f, v(d_f))$ (resp. $(-g, v(d_g))$ and $(-h, v(d_h))$) be the left and right endpoints, respectively, of the (possibly degenerate) segment in which the Newton polygon of P (resp. of Q) meets its support line of slope r. Then

$$v(c_i) + ri \geq v(c_e) + re = v(c_f) + rf$$
$$v(d_j) + rj \geq v(d_g) + rg = v(d_h) + rh$$

with strict inequality if $i \notin [e,f]$ or $j \notin [g,h]$. For each k,

$$\min_{i+j=k} \{v(c_i d_j) + rk\} \geq v(c_e) + re + v(d_g) + rg$$

and the inequality is strict in each of the following cases:

- $k \notin [f+h, e+g]$;
- $k = e+g$ and $i \neq e$;
- $k = f+h$ and $i \neq h$.

If we write $R = PQ$ and $R(z) = \sum a_k z^k$, it follows that

$$\min_k \{v(a_k) + rk\} \geq v(c_e) + re + v(d_g) + rg,$$

with equality for $k = f + h$ and $k = e + g$ but not for any $k \notin [f + h, e + g]$. It follows that the multiplicity of r as a slope of R is $e + g - (f + h) = (e - f) + (g - h)$, proving the desired result. □

Corollary 6.2.3. *Let $P(z)$ be a nonzero polynomial over $\mathbb{F}_q((t^{\mathbb{Q}}))$ which factors as a product $Q_1 \cdots Q_n$ of pure polynomials (e.g., linear polynomials). Then for each $r \in \mathbb{Q} \cup \{\infty\}$, the sum of the degrees of the Q_i, over those i for which Q_i has slope r, is equal to the multiplicity of r as a slope of P.*

6.3. Slope splittings. We now recall a special form of Hensel's lemma, which makes it possible to split polynomials by their slopes.

Definition 6.3.1. A subfield K of $\mathbb{F}_q((t^{\mathbb{Q}}))$ is *closed* under the valuation v if for any sequence $\{z_n\}_{n=0}^{\infty}$ such that $v(z_n - z_{n+1}) \to \infty$ as $n \to \infty$, there exists $z \in K$ such that $v(z_n - z) \to \infty$ as $n \to \infty$. For instance, $\mathbb{F}_q((t))$ is closed, as is any finite extension of $\mathbb{F}_q((t))$.

Lemma 6.3.2. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ closed under the valuation v. Let $P(z)$ be a nonzero polynomial over K, and choose $u \in \mathbb{Q}$ which does not occur as a slope of P. Then there exists a factorization $P = QR$, where Q is a polynomial over K with all slopes less than u, and R is a polynomial over K with all slopes greater than u.*

Proof. Pick $r, s \in \mathbb{Q}$ such that $r < s$ and the interval $[r, s]$ contains u but does not contain any slopes of P. Let S be the ring of formal sums $\sum_{j \in \mathbb{Z}} a_j z^j$ over K such that $v(a_j) + rj \geq 0$ for $j \geq 0$ and $v(a_j) + sj \geq 0$ for $j \leq 0$. Define the valuation v_u on S by the formula

$$v_u\left(\sum a_j z^j\right) = \min_j \{v(a_j) + uj\}.$$

Given $x = \sum a_j z^j \in S$, write $f(x) = \sum_{j>0} a_j z^j$, so that $f(f(x)) = f(x)$.

Write $P(z) = \sum_i c_i z^i$, put $d = \deg P$, let e be the unique integer that minimizes $v(c_e) + ue$, and put $x_0 = c_e^{-1} z^{-e} P(z) \in S$. Define the sequence $\{x_h\}_{h=0}^{\infty}$ by the recurrence $x_{h+1} = x_h(1 - f(x_h))$ for $h = 0, 1, \ldots$.

Put $\ell = v_u(x_0 - 1)$, so that $\ell > 0$. We now show by induction that $v_u(x_h - 1) \geq \ell$ and $v_u(f(x_h)) \geq (h+1)\ell$ for all h. The first inequality clearly implies the second for $h = 0$; given both inequalities for some h, we have

$$\begin{aligned} v_u(x_{h+1} - 1) &= v_u(x_h - x_h f(x_h) - 1) \\ &\geq \min\{v_u(x_h - 1), v_u(x_h) + v_u(f(x_h))\} \\ &\geq \min\{\ell, (h+1)\ell\} \\ &\geq \ell \end{aligned}$$

and

$$\begin{aligned} v_u(f(x_{h+1})) &= v_u(f(x_h - x_h f(x_h))) \\ &= v_u(f(x_h - f(x_h) - (x_h - 1)f(x_h))) \\ &= v_u(f(x_h) - f(f(x_h)) - f((x_h - 1)f(x_h))) \\ &= v_u(f((x_h - 1)f(x_h))) \\ &\geq v_u((x_h - 1)f(x_h)) \\ &\geq \ell + (h+1)\ell \\ &= (h+2)\ell. \end{aligned}$$

Thus the sequence $\{x_h\}$ converges to a limit $x \in S$.

By construction, $f(x) = 0$, so x has no positive powers of z. By induction on h, $z^e x_h$ has no negative powers of z for each h, so $z^e x$ also has no negative powers of z. Thus $z^e x$ is a polynomial in z of degree exactly e, and its slopes are all greater than or equal to s.

On the other hand, we have $x = x_0(1 - f(x_0))(1 - f(x_1)) \cdots$, so that $x_0 x^{-1}$ has only positive powers of z. However, $z^{e-d} x_0 x^{-1}$ has no positive powers of z, so $x_0 x^{-1}$ is a polynomial in z of degree exactly $d - e$, and its slopes are all less than or equal to r.

We thus obtain the desired factorization as $P = QR$ with $Q(z) = c_e x_0 x^{-1}$ and $R(z) = z^e x$. □

Corollary 6.3.3. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ closed under the valuation v. Then every monic polynomial P over K admits a unique factorization $Q_1 \cdots Q_n$ into monic polynomials, such that each Q_i is pure of some slope s_i, and $s_1 < s_2 < \cdots < s_n$.*

Proof. The existence of the factorization follows from Lemma 6.3.2; the uniqueness follows from unique factorization for polynomials over K and the additivity of multiplicities (Lemma 6.2.2). □

Definition 6.3.4. We call the factorization given by Corollary 6.3.3 the *slope factorization* of the polynomial P.

6.4. Slope splittings for twisted polynomials.

Remark 6.4.1. Throughout this section, we will use the fact that for K any subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$, the valuation v extends uniquely to any algebraic closure of K [18, Proposition II.3]. We do this for conceptual clarity; not doing so (at the expense of making the arguments messier and more computational) would not shed any light on how to compute with automatic series.

Lemma 6.4.2. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ closed under the valuation v. Let P be a monic additive polynomial over K, and let $Q_1 \cdots Q_n t^{p^d}$ be its slope factorization. Then $Q_n t^{p^d}$ is also additive.*

Proof. Let L be an algebraic closure of K. Let $s_1, \dots, s_n$ be the slopes of P, and let V be the roots of P in L; then the possible valuations of the nonzero elements of V are precisely $s_1, \dots, s_n$. Moreover, an element of V is a root of $Q_n t^{p^d}$ if and only if $v(x) \geq s_n$, and this subset of V is an $\mathbb{F}_p$-subspace of V. By Lemma 3.3.3, $Q_n t^{p^d}$ is also additive. □

In terms of twisted polynomials, we obtain the following analogue of the slope factorization.

Definition 6.4.3. Let $P(F)$ be a twisted polynomial over $\mathbb{F}_q((t^{\mathbb{Q}}))$. For $r \in \mathbb{Q}$, we say $P(F)$ is *pure of slope* r if P has nonzero constant term and the ordinary polynomial $P(F)(z)/z$ is pure of slope r. We conventionally say that any power of F is pure of slope ∞.

Proposition 6.4.4. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ closed under the valuation v, and let $P(F)$ be a monic twisted polynomial over K. Then there exists a factorization $P = Q_1 \cdots Q_n$ of P into monic twisted polynomials over K, in which each Q_i is pure of some slope.*

Proof. Let $R(z)$ be the highest finite slope factor in the slope factorization of $P(F)(z)$, times the slope ∞ factor (a power of z). By Lemma 6.4.2, $R(z)$ is additive, so we have $R(z) = Q(F)(z)$ for some twisted polynomial Q. By Lemma 6.1.5, we can factor $P = P_1 Q$ for some P_1 of lower degree than P; repeating the argument yields the claim. □

We can split further at the expense of enlarging q.

Proposition 6.4.5. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ closed under the valuation v, and let $P(F)$ be a monic twisted polynomial over K which is pure of slope 0. Then the polynomial $P(F)(z)$ factors completely (into linear factors) over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$, for some power q' of q.*

Proof. Write $P(F) = \sum_{i=0}^{d} c_i F^i$ with $c_d = 1$. Since P is pure of slope 0, we have $v(c_0) = 0$ and $v(c_i) \geq 0$ for $1 \leq i \leq d-1$.

Let $a_i \in \mathbb{F}_q$ be the constant coefficient of c_i; then for some power q' of q, the polynomial $\sum a_i z^{p^i}$ has p^d distinct roots in $\mathbb{F}_{q'}$. Let $r \in \mathbb{F}_{q'}$ be a nonzero root of $\sum a_i z^{p^i}$; then $P(F)(z+r)$ has one slope greater than 0 and all others equal to 0. The slope factorization of $P(F)(z+r)$ then has a linear factor; in other words, $P(F)(z)$ has a unique root $r' \in K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ with $v(r - r') > 0$. By the same argument, $P(F)(z)$ factors completely over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$, as desired. □

Corollary 6.4.6. *Let K be a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$, containing all fractional powers of t and closed under the valuation v, and let $P(F)$ be a monic twisted polynomial over K. Then for some power q' of q, there exists a factorization $P = Q_1 \cdots Q_n$ of P into monic* linear *twisted polynomials over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$.*

Proof. We may proceed by induction on $\deg P$; it suffices to show that if P is not linear, then it is a left multiple of some linear twisted polynomial over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ for some q'. By Proposition 6.4.4, we may reduce to the case where P is pure of some slope; by rescaling the polynomial $P(F)(z)$ (and using the fact that K contains all fractional powers of t), we may reduce to the case where P is pure of slope 0. By Proposition 6.4.5, $P(F)(z)$ then splits completely over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$ for some q'. Choose any one-dimensional $\mathbb{F}_p$-subspace of the set of roots of $P(F)(z)$; by Lemma 3.3.3, these form the roots of $Q(F)(z)$ for some monic linear twisted polynomial Q over $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q'}$. By Lemma 6.1.5, we can write $P = P_0 Q$ for some P_0; this completes the induction and yields the desired result. □

7. Proof of the main theorem: concrete approach

In this chapter, we study the properties of automatic power series more closely, with the end of giving a more down-to-earth proof (free of any dependence on Galois theory or the like) of the "algebraic implies automatic" implication of Theorem 4.1.3. In so doing, we introduce some techniques which may be of use in explicitly computing in the algebraic closure of $\mathbb{F}_q(t)$; however, we have not made any attempt to "practicalize" these techniques. Just how efficiently one can do such computing is a problem worthy of further study; we discuss this question briefly in the next chapter.

7.1. Transition digraphs of automata. We begin the chapter with a more concrete study of the automata that give rise to generalized power series.

Definition 7.1.1. Let M be a DFAO. Given a state $q_1 \in Q$, a state $q \in Q$ is said to be *reachable from* q_1 if $\delta^*(q_1, s) = q$ for some string $s \in \Sigma^*$, and *unreachable from* q_1 otherwise; if $q_1 = q_0$, we simply say that q is reachable or unreachable. Any state from which a state unreachable from q_0 can be reached must itself be unreachable from q_0. A DFAO with no unreachable states is said to be *minimal*; given any DFAO, one can remove all of its unreachable states to obtain a minimal DFAO that accepts the same language.

Definition 7.1.2. A state $q \in Q$ is said to be *relevant* if there exists a final state reachable from q, and *irrelevant* otherwise. Any state which is reachable from an irrelevant state must itself be irrelevant.

Definition 7.1.3. Let M be a DFA with input alphabet $\Sigma_b = \{0, \dots, b-1, .\}$. We say M is *well-formed* (resp. *well-ordered*) if the language accepted by M consists of the valid base b expansions of the elements of an arbitrary (resp. a well-ordered) subset of S_b.

The goal of this section is to characterize minimal well-ordered DFAs via their transition graphs; to do so, we use the following definitions. (By way of motivation, a connected undirected graph is called a "cactus" if each vertex of the graph lies on exactly one minimal cycle. In real life, the saguaro is a specific type of cactus indigenous to the southwest United States and northwest Mexico.)

Definition 7.1.4. A directed graph $G = (V, E)$ equipped with a distinguished vertex $v \in V$ is called a *rooted saguaro* if it satisfies the following conditions.

(a) Each vertex of G lies on at most one minimal cycle.
(b) There exist directed paths from v to each vertex of G.

In this case, we say that v is a *root* of the saguaro. (Note that a saguaro may have more than one root, because any vertex lying on the same minimal cycle as a root is also a root.) A minimal cycle of a rooted saguaro is called a *lobe*. An edge of a rooted saguaro is *cyclic* if it lies on a lobe and *acyclic* otherwise.

Definition 7.1.5. Let $G = (V, E)$ be a rooted saguaro. A *proper b-labeling* of G is a function $\ell : E \to \{0, \dots, b-1\}$ with the following properties.

(a) If $v, w, x \in V$ and $vw, vx \in E$, then $\ell(vw) \neq \ell(vx)$.
(b) If $v, w, x \in V$, $vw \in E$ lies on a lobe, and $vx \in E$ does not lie on a lobe, then $\ell(vw) > \ell(vx)$.

Theorem 7.1.6. *Let M be a DFA with input alphabet Σ_b, which is minimal and well-formed. Then M is well-ordered if and only if for each relevant postradix state q, the subgraph G_q of the transition graph consisting of relevant states reachable from q is a rooted saguaro with root q, equipped with a proper b-labeling.*

Proof. First suppose that M is well-ordered. Let q be a relevant postradix state of M; note that all transitions from q are labeled by elements of $\{0, \dots, b-1\}$, since a valid base b expansion cannot have two radix points. Suppose that q admits a cyclic transition by $s \in \{0, \dots, b-1\}$ and also admits a transition to a relevant state by $s' \neq s$. We will show that $s > s'$.

To see this, choose $w \in \Sigma^*$ of minimal length such that $\delta^*(q, sw) = q$. Since M is minimal, q is reachable, so we can choose $w_0 \in \Sigma^*$ such that $\delta^*(q_0, w_0) = q$. Since $\delta(q, s')$ is relevant, we can choose $w_1 \in \Sigma^*$ such that $\delta^*(q, s'w_1) \in F$. Then all of the strings

$$w_0 s' w_1, w_0 sws' w_1, w_0 swsws' w_1, \dots$$

are accepted by M; however, if $s' > s$, these form the valid base b expansions of an infinite decreasing sequence, which would contradict the fact that M is well-formed. Hence $s > s'$.

This implies immediately that a relevant postradix state cannot lie on more than one minimal cycle, so G_q is a rooted saguaro. Moreover, no two edges from the same vertex of G_q carry the same label, and what we just proved implies that any cyclic edge must carry a greater label than any other edge from the same vertex. Hence G_q carries a proper b-labeling.

Suppose conversely that each G_q is a rooted saguaro carrying a proper b-labeling, but assume by way of contradiction that the language accepted by M includes an infinite decreasing sequence $x_1, x_2, \dots$. We say the m-th digit of the base b expansion of x_i (counting from the left) is *static* if $x_i, x_{i+1}, \dots$ all have the same m-th digit. Then the expansion of each x_i begins with an initial segment (possibly empty) of static digits, and the number of static digits tends to infinity with i. There exists a unique infinite sequence $s_1, s_2, \dots$ of elements of Σ such that each initial segment of static digits occurring in the expansion of some x_i has the form $s_1 \cdots s_m$ for some m (depending on i).

The number of preradix digits in the expansion of x_i is at most the corresponding number for x_1, so the sequence $s_1, s_2, \dots$ must include one (and only one) radix point. Define $q_m = \delta^*(q_0, s_1 \cdots s_m)$; then each q_m is relevant, and q_m is postradix for m sufficiently large. Moreover, only finitely many of the postradix transitions from q_m to q_{m+1} can be acyclic, as otherwise some such transition would repeat, but then would visibly be part of a cycle.

Choose x_i in the decreasing sequence whose first m digits are all static, for m large enough that q_m is postradix and the transition from q_n to q_{n+1} is cyclic for all $n \geq m$ (again, this amounts to taking i sufficiently large). Let $t_1 t_2 \cdots \in \Sigma^*$ denote the base b expansion of x_i. Since $x_{i+1} < x_i$, there exists a smallest integer $n > m$ such that $s_n \neq t_n$, and that integer n satisfies $s_n < t_n$. However, the transition from q_n to q_{n+1} is cyclic, and so the inequality $s_n < t_n$ violates the definition of a proper b-labeling. This contradiction means that there cannot exist an infinite decreasing subsequence, so M is well-ordered, as desired. □

7.2. Arithmetic for well-ordered automata. We next verify directly that the set of automatic series is a ring; this follows from Theorem 4.1.3 and Lemma 3.2.5, but giving a direct proof will on one hand lead to a second proof of Theorem 4.1.3, and on the other hand suggest ways to implement computations on automatic series in practice. (However, we have not made any attempt here to optimize the efficiency of the computations; this will require further study.)

We first note that adding automatic series is easy.

Lemma 7.2.1. *Let $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ be p-automatic (resp. p-quasi-automatic). Then $x + y$ is p-automatic (resp. p-quasi-automatic).*

Proof. The claim for p-quasi-automatic series follows from the claim for p-automatic series by Lemma 2.3.6, so we may as well assume that x, y are p-automatic. Write $x = \sum x_i t^i$ and $y = \sum y_i t^i$; then by assumption, the functions $i \mapsto x_i$ and $i \mapsto y_i$ on S_p are p-automatic. Hence the function $i \mapsto (x_i, y_i)$ is also p-automatic, as then is the function $i \mapsto x_i + y_i$. This yields the claim. □

We next tackle the stickier subject of multiplication of automatic series.

Lemma 7.2.2. *Let $x, y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ be p-automatic (resp. p-quasi-automatic). Then xy is p-automatic (resp. p-quasi-automatic).*

Beware that this proof works primarily with *reversed* base p expansions; the notions of leading and trailing zeroes will be in terms of the reversed expansions, so leading zeroes are in the *least* significant places.

Proof. Again, it suffices to treat the automatic case. Write each of x and y as an $\mathbb{F}_q$-linear combination of generalized power series of the form $\sum_{i \in S} t^i$ for some $S \subset S_p$; by Lemma 7.2.1, if the product of two series of this form is always p-automatic, then so is xy.

That is, we may assume without loss of generality that $x = \sum_{i \in A_1} t^i$ and $y = \sum_{i \in A_2} t^i$. Let S be the subset of $\Sigma_p^* \times \Sigma_p^*$ consisting of pairs (w_1, w_2) with the following properties.

(a) w_1 and w_2 have the same length.
(b) w_1 and w_2 each end with 0.
(c) w_1 and w_2 each have a single radix point, and both are in the same position.
(d) After removing leading and trailing zeroes, w_1 and w_2 become the reversed valid base p expansions of some $i, j \in S_p$.
(e) The pair (i, j) belongs to $A_1 \times A_2$.

By (a), we may view S as a language over $\Sigma_p \times \Sigma_p$; it is straightforward to verify that this language is in fact regular. Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA accepting S, with $\Sigma = \Sigma_p \times \Sigma_p$.

Define an NFA $M' = (Q', \Sigma', \delta', q_0', F')$, in which δ' takes multiset values, as follows. Put $Q' = Q \times \{0, 1\}$ and $\Sigma' = \Sigma_p$. For $(q, i) \in Q'$ and $s \in \{0, \dots, p-1\}$, we include $(q', 0)$ (resp. $(q', 1)$) in $\delta'((q, i), s)$ once for each pair $(t, u) \in \{0, \dots, p-1\} \times \{0, \dots, p-1\}$ with $t+u+i < p$ (resp. $t+u+i \geq p$) and $t + u + i \equiv s \pmod{p}$ such that $\delta(q, (t, u)) = q'$; for $(q, i) \in Q'$ and s equal to the radix point, we include (q', i) in $\delta((q, i), s)$ if $\delta(q, (s, s)) = q'$ (and we never include $(q', 1 - i)$). Put $q_0' = (q_0, 0)$ and put $F' = F \times \{0\}$.

Suppose w is a string which, upon removal of leading and trailing zeroes, becomes the reversed valid base p expansion of some $z \in S_p$. Then the number of accepting paths of w in M' is equal to the number of pairs $(w_1, w_2) \in S$ which sum to w *with its leading and trailing zeroes* under ordinary base p addition with carries. By Lemma 2.2.2, taking this number modulo p yields a finite-state function.

Suppose further that w begins with m leading zeroes, for m greater than the number of states of M. We claim that for any pair $(w_1, w_2) \in S$ which sums to w, both w_1 and w_2 must begin with a leading zero. Namely, if this were not the case, then in processing $(w_1, w_2) \in S$ under M, some state must be repeated within the first m digits. Let (b_1, b_2) be the strings that lead to the first arrival at such repeated state, let (m_1, m_2) be the strings between the first and second arrivals, and let (e_1, e_2) be the remaining strings. Then

$$b_i e_i, b_i m_i e_i, b_i m_i m_i e_i, \dots,$$

represent the reversed base p expansions (with possible trailing zeroes, but no leading zeroes) of some elements $z_{0i}, z_{1i}, \dots$ of A_i. Moreover, the numbers $z_{0i}, z_{1i}, \dots$ are all distinct: if b_i is nonempty, then b_i begins with a nonzero digit, while if b_i is empty, then m_i begins with a nonzero digit.

We next verify that $z_{j0} + z_{j1} = z$ for each j. We are given this assertion for $j = 1$; in doing that addition, the stretch during which w_1 and w_2 are added begins with an incoming carry and ends with an outgoing carry. Moreover, all digits produced before and during the stretch are zeroes. Thus we may remove this stretch, or repeat it at will, without changing the base p number represented by the sum (though the number of leading zeroes will change).

Since $z_{j0} + z_{j1} = z$ for all j, one of the sequences $z_{0i}, z_{1i}, \dots$ must be strictly decreasing. This yields a contradiction, implying that both w_1 and w_2 had to begin with leading zeroes. We conclude from this that the number of accepting paths of w in M' is preserved by adding a leading zero to w provided that w already has m leading zeroes.

It follows that the function that, given the reversed valid base p expansion of a number $k \in S_p$, computes the mod p reduction of the number of ways to write $k = i + j$ with $i \in A_1$ and $j \in A_2$, is a finite-state function: we may compute it by appending m leading zeroes and one trailing zero to the reversed expansion and then running the result through M'. Thus xy is p-automatic, as desired. ☐

Division seems even more complicated to handle directly (though we suspect it is possible to do so); we treat it here with an indirect approach (via the "automatic implies algebraic" direction of Theorem 4.1.3).

Lemma 7.2.3. *If $x \in \mathbb{F}_q(t)$, then x (viewed as an element of $\mathbb{F}_q((t^{\mathbb{Q}}))$) is p-automatic.*

Proof. There is no loss of generality in assuming $x \in \mathbb{F}_q[\![t]\!]$. Writing $x = \sum_{i=0}^{\infty} c_i t^i$, we see that the sequence $\{c_i\}$ is linear recurrent over $\mathbb{F}_q$, hence eventually periodic. By [2, Theorem 5.4.2], x is p-automatic. ☐

Proposition 7.2.4. *The set of p-quasi-automatic series is a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ contained in the integral closure of $\mathbb{F}_q(t)$.*

Proof. Let S be the set of p-quasi-automatic series. By Lemmas 7.2.1 and 7.2.2, S is a subring of $\mathbb{F}_q((t^{\mathbb{Q}}))$. By Lemma 7.2.3, S contains $\mathbb{F}_q(t)$; by Proposition 5.2.7, each element of S is algebraic over $\mathbb{F}_q(t)$. Hence given $x \in S$, there exists a polynomial $P(z) = c_0 + c_1 z + \cdots + c_n z^n$ over $\mathbb{F}_q(t)$ with $P(x) = 0$, and we may assume without loss of generality that $c_0, c_n \neq 0$. We can then write

$$x^{-1} = -c_0^{-1}(c_1 + c_2 x + \cdots + c_n x^{n-1}),$$

and the right side is contained in S. We conclude that S is closed under taking reciprocals, and hence is a subfield of $\mathbb{F}_q((t^{\mathbb{Q}}))$ contained in the integral closure of $\mathbb{F}_q(t)$, as desired. □

7.3. Newton's algorithm. To complete the "concrete" proof of the "algebraic implies automatic" direction of Theorem 4.1.3, we must explain why the field of p-quasi-automatic series is closed under extraction of roots of polynomials. The argument we give below implicitly performs a positive characteristic variant of Newton's algorithm; most of the work has already been carried out in Chapter 6. (By contrast, a direct adaptation of Newton's algorithm to generalized power series gives a transfinite process; see [12, Proposition 1].)

Before proceeding further, we explicitly check that the class of p-quasi-automatic series is closed under the formation of Artin-Schreier extensions.

Lemma 7.3.1. *For any p-quasi-automatic $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ supported within $(-\infty, 0)$, there exists a p-quasi-automatic series $y \in \mathbb{F}_q((t^{\mathbb{Q}}))$ such that $y^p - y = x$.*

Proof. We can take

$$y = x^{1/p} + x^{1/p^2} + \cdots$$

once we show that this generalized power series is p-quasi-automatic. There is no loss of generality in assuming that xt^a is p-automatic for some nonnegative integer a; in fact, by decimating, we may reduce to the case where $a = 1$.

Write $y = \sum y_i t^i$. Since

$$y_i = x_{ip} + x_{ip^2} + \cdots,$$

for any fixed j, the series

$$\sum_{i < -p^{-j}} y_i t^i$$

is p-automatic. Also, for $i \in [-1, 0)$, the sequence

$$x_i, x_{i/p}, x_{i/p^2}, \ldots$$

is generated by inputting the base p expansions of $1+i, 1+i/p, 1+i/p^2, \dots$ into a fixed finite automaton; hence there exist integers m and n such that for any $i \in [-1,0)$, $y_{ip^{-m}} = y_{ip^{-n}}$.

From this we can construct a finite automaton that, upon receiving $1+i$ at input, returns y_i. Namely, the automaticity of $\sum_{i<-p^{-n}} y_i t^i$ gives an automaton that returns y_i if $i < -p^{-n}$. If $i \geq -p^{-n}$, then $1+i \geq 1-p^{-n}$, so the base p expansion begins with n digits equal to $p-1$, and conversely. We can thus loop back to wherever we were after m digits equal to $p-1$; since $y_{ip^{-m}} = y_{ip^{-n}}$, we end up computing the right coefficient. Hence y is p-quasi-automatic, as desired. □

Lemma 7.3.2. *Let $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ be the closure, under the valuation v, of the field of p-quasi-automatic series. Then for any $a, b \in R_q$ with $a \neq 0$, the equation*

$$z^p - az = b$$

has p distinct solutions in $R_{q'}$ for some power q' of q.

Proof. We first check the case $b = 0$, i.e., we show that $z^{p-1} = a$ has $p-1$ distinct solutions in $R_{q'}$ for some q'. Write $a = a_0 t^i (1+u)$, where $a_0 \in \mathbb{F}_q$, $i \in \mathbb{Q}$, and $v(u) > 0$. Choose q' so that a_0 has a full set of $(p-1)$-st roots in $\mathbb{F}_{q'}$; we can then take

$$z = a_0^{1/(p-1)} t^{i/(p-1)} \sum_{j=0}^{\infty} \binom{1/(p-1)}{j} u^j$$

for any $(p-1)$-st root $a_0^{1/(p-1)}$ of a_0 .

We now proceed to the case of general b. By the above argument, we can reduce to the case $a = 1$. We can then split $b = b_- + b_+$, where b_- is supported on $(-\infty, 0)$ and b_+ is supported on $[0, \infty)$, and treat the cases $b = b_-$ and $b = b_+$ separately. The former case is precisely Lemma 7.3.1. As for the latter case, let b_0 be the constant coefficient of b_+, and choose q' so that the equation $z^p - z = b_0$ has distinct roots $c_1, \dots, c_p \in \mathbb{F}_{q'}$. We may then take

$$z = c_i - \sum_{j=0}^{\infty} (b_+ - b_0)^{p^j}$$

to obtain the desired solutions. □

Proposition 7.3.3. *Let $R_q \subset \mathbb{F}_q((t^{\mathbb{Q}}))$ be the closure, under the valuation v, of the field of p-quasi-automatic series, and let R be the union of the rings $R_{q'}$ over all powers q' of q. Then R (which is also a field) is algebraically closed.*

Proof. By Lemma 3.3.4, it suffices to show that for every monic twisted polynomial $P(F)$ over R_q, the polynomial $P(F)(z)$ factors completely over

$R_{q'}$ for some q'. Since R_q is perfect, we may factor off F on the right if it appears, to reduce to the case where P has nonzero constant coefficient, or equivalently (by Lemma 6.1.4) where $P(F)(z)$ has no repeated roots.

By Corollary 6.4.6, we can write $P = Q_1 \cdots Q_n$ for some monic linear twisted polynomials $Q_1, \dots, Q_n$ over $R_{q'}$ for some q'. Write $Q_i = F - c_i$ (where $c_i \neq 0$); the process of finding roots of $P(F)(z)$ can then be described as the process of finding solutions of the system of equations

$$\begin{aligned} z_1^p - c_1 z_1 &= 0 \\ z_2^p - c_2 z_2 &= z_1 \\ &\vdots \\ z_n^p - c_n z_n &= z_{n-1} \end{aligned}$$

(the roots of $P(F)(z)$ being precisely the possible values of z_n). By repeated applications of Lemma 7.3.2, the system has p^n distinct solutions, and so $P(F)(z)$ splits completely as desired. □

At this point, we can now deduce that "algebraic implies automatic" in much the same manner as in Proposition 5.2.7. This means in particular that again we will need to invoke Christol's theorem.

Proposition 7.3.4. *Let $x = \sum x_i t^i \in \mathbb{F}_q((t^{\mathbb{Q}}))$ be a generalized power series which is algebraic over $\mathbb{F}_q(t)$. Then x is p-quasi-automatic.*

Proof. There exists a polynomial $P(z)$ over $\mathbb{F}_q(t^{1/p^m})$, for some nonnegative integer m, such that P has x as a root with multiplicity 1; by replacing x with x^{p^m}, we may reduce without loss of generality to the case where $m = 1$. Choose $c \in \mathbb{Q}$ such that $c > v(x - x')$ for any root $x' \neq x$ of P.

By Proposition 7.3.3, there exists a power q' of q and a p-quasi-automatic series y over $\mathbb{F}_{q'}((t^{\mathbb{Q}}))$ such that $v(x - y) \geq c$. The polynomial $P(z + y)$ then has exactly one root of slope at least c, namely $x - y$.

By Proposition 5.1.2, y is algebraic over $\mathbb{F}_q(t)$. Let K be the finite extension of $\mathbb{F}_{q'}((t))$ obtained by adjoining y. Then K is complete under v; by Corollary 6.3.3, we may split off the unique factor of $P(z + y)$ of slope at least c. In other words, $x - y \in K$, and so $x \in K$.

At this point the argument parallels that of Proposition 5.2.7. Let m be the degree of the minimal polynomial of y over $\mathbb{F}_q(t)$. For $j = 0, \dots, m-1$, write

$$y^{pj} = \sum_{i=0}^{m-1} a_{ij} y^i$$

with $a_{ij} \in \mathbb{F}_q((t))$; then the a_{ij} are algebraic over $\mathbb{F}_q(t)$. Choose n minimal such that $x, x^p, \dots, x^{p^n}$ are linearly dependent over $\mathbb{F}_q((t))$. Write $x^{p^j} =$

$\sum_{i=0}^{m-1} b_{ij} y^i$ with $b_{ij} \in \mathbb{F}_q((t))$; we then have the equations

$$b_{i(j+1)} = \sum_{l=0}^{m-1} b_{lj}^p a_{il} \qquad (j = 0, \dots, n-1).$$

Let $c_0 x + \cdots + c_n x^{p^n} = 0$ be a linear relation over $\mathbb{F}_q((t))$, which we may normalize by setting $c_0 = 1$; then the c_i are algebraic over $\mathbb{F}_q(t)$. Also, writing $x = -c_1 x^p - \cdots - c_n (x^{p^{n-1}})^p$, we have

$$\begin{aligned}
\sum_{i=0}^{m-1} b_{i0} y^i &= \sum_{j=0}^{n-1} -c_{j+1} (x^{p^j})^p \\
&= \sum_{l=0}^{m-1} \sum_{j=0}^{n-1} -c_{j+1} b_{lj}^p y^{pl} \\
&= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{lj}^p a_{il} y^i,
\end{aligned}$$

and hence

$$b_{i0} = \sum_{j=0}^{n-1} \sum_{l=0}^{m-1} -c_{j+1} b_{lj}^p a_{il}.$$

We thus have a system of equations in the b_{ij} as in Lemma 3.3.5 (with B equal to the identity matrix); this allows us to conclude that each b_{ij} is algebraic over $\mathbb{F}_q(t)$.

By Christol's theorem (Theorem 4.1.1), each $b_{ij} \in \mathbb{F}_q((t))$ is p-automatic. Hence $x = \sum_{i=0}^{m-1} b_{i0} y^i$ is p-quasi-automatic, as desired. □

8. Further questions

We end with some further questions about automata and generalized power series, of both an algorithmic and a theoretical nature.

8.1. Algorithmics of automatic series. It seems that one should be able to make explicit calculations in the algebraic closure of $\mathbb{F}_q(t)$ using automatic power series; we have not made any systematic attempt to do so, but it is worth recording some observations here for the benefit of anyone considering doing so in the future.

The issue of computing in the algebraic closure of $\mathbb{F}_q(t)$ using generalized power series resembles that of computing in the algebraic closure of $\mathbb{Q}$ using complex approximations of algebraic numbers, and some lessons may be profitably drawn from that case. In particular, it may be worth computing "approximately" and not exactly with automatic power series, in a form of "interval arithmetic".

In contrast with the $\mathbb{Q}$-analogue, however, there are two ways to truncate a computation with automata: one can ignore large powers of t (analogous to working with a complex approximation of an algebraic number), but one can also prune the automata by ignoring states that cannot be reached in some particular number of steps from the initial state. The latter may be crucial for making multiplication of automatic series efficient, as the methods we have described seem to entail exponential growth in the number of states over the course of a sequence of arithmetic operations. Further analysis will be needed, however, to determine how much pruning one can get away with, and how easily one can recover the missing precision in case it is needed again.

Our techniques seem to depend rather badly on the size of the finite field $\mathbb{F}_q$ under consideration, but it is possible this dependence can be ameliorated. For instance, some of this dependence (like the complexity of a product) is really not on q but on the characteristic p, and so is not so much of an issue when working over a field of small characteristic (as long as one decomposes everything over a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$). Also, it may be possible to work even in large characteristic by writing everything in terms of a small additive basis of the finite field (e.g., for $\mathbb{F}_p$, use the powers of 2 less than p), at least if one is willing to truncate as in the previous paragraph.

One additional concern that arises when the characteristic is not small is that our method for extracting roots of polynomials requires working with additive polynomials. Given an ordinary polynomial $P(z)$ of degree n, one easily obtains an additive polynomial of degree at most p^n which has $P(z)$ as a factor (by reducing $z, z^p, z^{p^2}, \dots$ modulo P); however, the complexity of the coefficients of the new polynomial grows exponentially in n. It would be of some interest to develop a form of Newton's algorithm to deal directly with ordinary polynomials.

8.2. Multivariate series and automata. We conclude by mentioning a multivariate version of Christol's theorem and conjecturing a generalized power series analogue. Following [2, Chapter 14], we restrict our notion of "multivariate" to "bivariate" for notational simplicity, and leave it to the reader's imagination to come up with full multivariate analogues.

For b an integer greater than 1, a *valid pair of base b expansions* is a pair of strings $(s_1 \dots s_n, t_1 \dots t_n)$ of equal length over the alphabet $\Sigma = \{0, \dots, b-1, .\}$ such that s_1 and t_1 are not both 0, s_n and t_n are not both 0, each of the strings $s_1 \dots s_n$ and $t_1 \dots t_n$ contains exactly one radix point, and those radix points occur at the same index k. We define the *value* of such a pair to be the pair

$$\left(\sum_{i=1}^{k-1} s_i b^{k-1-i} + \sum_{i=k+1}^{n} s_i b^{k-i}, \quad \sum_{i=1}^{k-1} t_i b^{k-1-i} + \sum_{i=k+1}^{n} t_i b^{k-i}\right);$$

then the value function gives a bijection between the set of valid pairs of base b expansions and $S_b \times S_b$. Let s denote the inverse function. (Note that it may happen that one string or the other has some leading and/or trailing zeroes, since we are forcing them to have the same length.)

We may identify pairs of strings over Σ_b of equal length with strings over $\Sigma_b \times \Sigma_b$ in the obvious fashion, and under this identification, the set of valid pairs of base b expansions are seen to form a regular language. With that in mind, we declare a function $f : S_b \times S_b \to \Delta$ to be *b-automatic* if there exists a DFAO with input alphabet $\Sigma = \Sigma_b \times \Sigma_b$ and output alphabet Δ such that for any pair $(v, w) \in S_b \times S_b$, $f(v, w) = f_M(s(v, w))$. We declare a double sequence $\{a_{i,j}\}_{i,j=0}^{\infty}$ over Δ to be b-automatic if for some $\star \notin \Delta$, the function $f : S_b \times S_b \to \Delta \cup \{\star\}$ given by

$$f(v, w) = \begin{cases} a_{v,w} & v, w \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$

is b-automatic.

In this language, the bivariate version of Christol's theorem is the following result, due to Salon [16], [17] (see also [2, Theorem 14.4.1]). Here $\mathbb{F}_q(t, u)$ denotes the fraction field of the polynomial ring $\mathbb{F}_q[t, u]$; this field is contained in the fraction field of the power series ring $\mathbb{F}_q[\![t, u]\!]$.

Theorem 8.2.1. *Let q be a power of the prime number p, and let $\{a_{i,j}\}_{i,j=0}^{\infty}$ be a double sequence over $\mathbb{F}_q$. Then the double series $\sum_{i,j=0}^{\infty} a_{i,j} t^i u^j \in \mathbb{F}_q[\![t, u]\!]$ is algebraic over $\mathbb{F}_q(t, u)$ if and only if the double sequence $\{a_{i,j}\}_{i,j=0}^{\infty}$ is p-automatic.*

To even formulate a generalized power series analogue of Theorem 8.2.1, we must decide what we mean by "generalized power series in two variables". The construction below is natural enough, but we are not aware of a prior appearance in the literature.

Let G be a *partially ordered* abelian group (written additively) with identity element 0; that is, G is an abelian group equipped with a binary relation $>$ such that for all $a, b, c \in G$,

$$a \not> a$$
$$a > b, b > c \Rightarrow a > c$$
$$a > b \Leftrightarrow a + c > b + c.$$

Let P be the set of $a \in G$ with $a > 0$; P is again called the *positive cone* of G. We write $a \geq b$ to mean $a > b$ or $a = b$, and $a \leq b$ to mean $b \geq a$.

Then one has the following analogue of Lemma 3.1.2, whose proof we leave to the reader.

Lemma 8.2.2. *Let S be a subset of G. Then the following two conditions are equivalent.*

(a) *Every nonempty subset of S has at least one, but only finitely many, minimal elements. (An element $x \in S$ is* minimal *if $y \in S$ and $y \leq x$ imply $y = x$. Note that "minimal" does not mean "smallest".)*

(b) *Any sequence $s_1, s_2, \ldots$ over S contains an infinite weakly increasing subsequence $s_{i_1} \leq s_{i_2} \leq \cdots$.*

A subset S of G is *well-partially-ordered* if it satisfies either of the equivalent conditions of Lemma 8.2.2. (This condition has cropped up repeatedly in combinatorial situations; see [14] for a survey, if a somewhat dated one.) Then for any ring R, the set of functions $f : G \to R$ which have well-partially-ordered support forms a ring under termwise addition and convolution.

For $G = \mathbb{Q} \times \mathbb{Q}$, let $R((t^{\mathbb{Q}}, u^{\mathbb{Q}}))$ denote the ring just constructed; we refer to its elements as "generalized double Laurent series". Then by analogy with Theorem 4.1.3, we formulate the following conjecture.

Conjecture 8.2.3. *Let q be a power of the prime p, and let $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{F}_q$ be a function whose support S is well-partially-ordered. Then the corresponding generalized double Laurent series $\sum_{i,j} f(i,j) t^i u^j \in \mathbb{F}_q((t^{\mathbb{Q}}, u^{\mathbb{Q}}))$ is algebraic over $\mathbb{F}_q(t,u)$ if and only if the following conditions hold.*

(a) *For some positive integers a and b, the set $aS + b = \{(ai + b, aj + b) : (i,j) \in S\}$ is contained in $S_p \times S_p$.*

(b) *For some a, b for which (a) holds, the function $f_{a,b} : S_p \times S_p \to \mathbb{F}_q$ given by $f_{a,b}(x,y) = f((x-b)/a, (y-b)/a)$ is p-automatic.*

Moreover, if these conditions hold, then $f_{a,b}$ is p-automatic for any nonnegative integers a, b for which (a) holds.

An affirmative answer to Conjecture 8.2.3 would imply that if the generalized double Laurent series $\sum_{i,j} c_{i,j} t^i u^j$ is algebraic over $\mathbb{F}_q(t,u)$, then the diagonal series $\sum_i c_{i,i} t^i$ is algebraic over $\mathbb{F}_q(t)$; for ordinary Laurent series, this result is due to Deligne [6].

Deligne's result actually allows an arbitrary field of positive characteristic in place of $\mathbb{F}_q$, but his proof is in the context of sophisticated algebro-geometric machinery (vanishing cycles in étale cohomology); a proof of Deligne's general result in the spirit of automata-theoretic methods was given by Sharif and Woodcock [19]. It may be possible to state and prove an analogous assertion in the generalized Laurent series setting by giving a suitable multivariate extension of the results of [11].

References

[1] S. ABHYANKAR, *Two notes on formal power series.* Proc. Amer. Math. Soc. **7** (1956), 903–905.
[2] J.-P. ALLOUCHE, J. SHALLIT, *Automatic Sequences: Theory, Applications, Generalizations.* Cambridge Univ. Press, 2003.
[3] C. CHEVALLEY, *Introduction to the Theory of Algebraic Functions of One Variable.* Amer. Math. Soc., 1951.
[4] G. CHRISTOL, *Ensembles presque periodiques k-reconnaissables.* Theoret. Comput. Sci. **9** (1979), 141–145.
[5] G. CHRISTOL, T. KAMAE, M. MENDÈS FRANCE, G. RAUZY, *Suites algébriques, automates et substitutions.* Bull. Soc. Math. France **108** (1980), 401–419.
[6] P. DELIGNE, *Intégration sur un cycle évanescent.* Invent. Math. **76** (1984), 129–143.
[7] H. FURSTENBERG, *Algebraic functions over finite fields.* J. Alg. **7** (1967), 271–277.
[8] H. HAHN, *Über die nichtarchimedische Größensysteme* (1907). Gesammelte Abhandlungen I, Springer-Verlag, 1995.
[9] D.R. HAYES, *A brief introduction to Drinfel'd modules.* The Arithmetic of Function Fields (edited by D. Goss, D.R. Hayes, and M.I. Rosen), 1–32, de Gruyter, 1992.
[10] I. KAPLANSKY, *Maximal fields with valuations.* Duke Math. J. **9** (1942), 303–321.
[11] K.S. KEDLAYA, *The algebraic closure of the power series field in positive characteristic.* Proc. Amer. Math. Soc. **129** (2001), 3461–3470.
[12] K.S. KEDLAYA, *Power series and p-adic algebraic closures. J. Number Theory* **89** (2001), 324–339.
[13] K.S. KEDLAYA, *Algebraic generalized power series and automata.* arXiv preprint math. AC/0110089, 2001.
[14] J.B. KRUSKAL, *The theory of well-quasi-ordering: a frequently discovered concept.* J. Comb. Theory Ser. A **13** (1972), 297–305.
[15] D.S. PASSMAN, *The Algebraic Structure of Group Rings.* Wiley, 1977.
[16] O. SALON, *Suites automatiques à multi-indices et algébricité.* C.R. Acad. Sci. Paris Sér. I Math. **305** (1987), 501–504.
[17] O. SALON, *Suites automatiques à multi-indices* (with an appendix by J. Shallit). Sem. Théorie Nombres Bordeaux **4** (1986–1987), 1–27.
[18] J.-P. SERRE, *Local Fields* (translated by M.J. Greenberg). Springer-Verlag, 1979.
[19] H. SHARIF, C.F. WOODCOCK, *Algebraic functions over a field of positive characteristic and Hadamard products.* J. London Math. Soc. **37** (1988), 395–403.

Kiran S. KEDLAYA
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
E-mail : kedlaya@math.mit.edu
URL: http://math.mit.edu/~kedlaya