

# *Algebra & Number Theory*

Volume 11

2017

No. 3

**Automatic sequences and curves  
over finite fields**

Andrew Bridy



# Automatic sequences and curves over finite fields

Andrew Bridy

We prove that if  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$  is an algebraic power series of degree  $d$ , height  $h$ , and genus  $g$ , then the sequence  $\mathbf{a}$  is generated by an automaton with at most  $q^{h+d+g-1}$  states, up to a vanishingly small error term. This is a significant improvement on previously known bounds. Our approach follows an idea of David Speyer to connect automata theory with algebraic geometry by representing the transitions in an automaton as twisted Cartier operators on the differentials of a curve.

## 1. Introduction

Our starting point is the following well-known theorem of finite automata theory.

**Theorem 1.1** [Christol 1979; Christol et al. 1980]. *The power series*

$$y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$$

is algebraic over  $\mathbb{F}_q(x)$  if and only if the sequence  $\mathbf{a}$  is  $q$ -automatic.

Christol's theorem establishes a dictionary between automatic sequences and number theory in positive characteristic. The purpose of this paper is to investigate how complexity translates across this dictionary. A secondary purpose is to demonstrate an intimate connection between automatic sequences and the algebraic geometry of curves.

We take the complexity of a sequence  $\mathbf{a}$  to be *state complexity*. Let  $N_q(\mathbf{a})$  denote the number of states in a minimal  $q$ -automaton that generates  $\mathbf{a}$  in the reverse-reading convention (this will be defined precisely in Section 2). If  $y$  is algebraic over  $k(x)$ , let the *degree*  $\deg y$  be the usual field degree  $[k(x)[y] : k(x)]$  and the *height*  $h(y)$  be the minimal  $x$ -degree of a bivariate polynomial  $f(x, T) \in k[x, T]$  such that  $f(x, y) = 0$ . The *genus* of  $y$  will be the genus of the normalization of the projective closure of the affine plane curve defined by the minimal polynomial of  $y$ .

*MSC2010*: primary 11B85; secondary 11G20, 14H05, 14H25.

*Keywords*: automatic sequences, formal power series, algebraic curves, finite fields.

We bound the complexity of  $\mathbf{a}$  in terms of the degree, height, and genus of  $y$ . In [Section 2](#) we review some known lower bounds. Our main result is the following upper bound.

**Theorem 1.2.** *Let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$  be algebraic over  $\mathbb{F}_q(x)$  of degree  $d$ , height  $h$ , and genus  $g$ . Then*

$$N_q(\mathbf{a}) \leq (1 + o(1))q^{h+d+g-1}.$$

The  $o(1)$  term tends to 0 for large values of  $q$ ,  $h$ ,  $d$ , or  $g$ .

All previous upper bounds are much larger. These are usually stated in terms of the  $q$ -kernel of  $\mathbf{a}$ , which can be described as the orbit of a certain semigroup acting on the series  $y$  and is in bijection with a minimal automaton that outputs  $\mathbf{a}$  (see [Theorem 2.2](#)). The best previous bound is due to Fresnel, Koskas, and de Mathan [[2000](#), [Theorem 2.2](#)] who show that

$$N_q(\mathbf{a}) \leq q^{qd(h(2d^2-2d+1)+C)}, \quad (1.3)$$

for some  $C = C(q)$  that they do not seem to compute exactly. Adamczewski and Bell [[2012](#), p. 383] prove a bound that is roughly  $q^{d^4h^2p^{5d}}$ , where  $p = \text{char } \mathbb{F}_q$ . Earlier, Derksen [[2007](#), [Proposition 6.5](#)] showed a special case of the bound of Adamczewski and Bell for rational functions. Harase [[1988](#); [1989](#)] proved a larger bound using essentially the same technique. It should be noted that some of these results hold in more generality than the setting of this paper; the techniques of Adamczewski, Bell, and Derksen apply to power series in several variables over infinite ground fields of positive characteristic (with appropriate modifications).

In [Proposition 3.14](#) we show that [Theorem 1.2](#) is qualitatively sharp for the power series expansions of rational functions, in that it is sharp if we replace the  $o(1)$  term by 0. There are some special cases where the bound can be improved. For example, an easy variation of our main argument shows that if  $y dx$  is a holomorphic differential on the curve defined by the minimal polynomial of  $y$ , then  $N_q(\mathbf{a}) \leq q^{d+g-1}$  (see [Example 4.3](#)). It is also possible to give a coarser estimate that is independent of  $g$ , which shows that [Theorem 1.2](#) compares favorably to the work of Fresnel et al., even when the genus is as large as possible:

**Corollary 1.4.** *Under the hypotheses of [Theorem 1.2](#),  $N_q(\mathbf{a}) \leq (1 + o(1))q^{hd}$ .*

*Proof.* Let  $X$  be the curve defined by the minimal polynomial of  $y$ . Observe that  $d$  is the degree of the map  $\pi_x : X \rightarrow \mathbb{P}^1$  that projects on the  $x$ -coordinate. Likewise,  $h$  is the degree of the projection map  $\pi_y : X \rightarrow \mathbb{P}^1$ . Therefore  $g \leq (d-1)(h-1)$  by Castelnuovo's inequality (actually, a special case originally due to Riemann, see [[Stichtenoth 2009](#), [Corollary 3.11.4](#)]).  $\square$

Though the reverse-reading convention is the natural one to use in the context of algebraic series, our approach also gives an upper bound on the state complexity of forward-reading automata via a dualizing argument. Let  $N_q^f(\mathbf{a})$  denote the minimal number of states in a forward-reading automaton that generates the sequence  $\mathbf{a}$ , and let  $y$  be as in [Theorem 1.2](#).

**Theorem 1.5.** 
$$N_q^f(\mathbf{a}) \leq q^{h+2d+g-1}.$$

To our knowledge, there are no previous bounds on forward-reading complexity in this context except for the well-known observation that  $N_q^f(\mathbf{a}) \leq q^{N_q(\mathbf{a})}$  (see [Proposition 2.4](#)).

The key idea in our argument is to recast finite automata in the setting of algebraic geometry. If  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n$  is algebraic, then it lies in the function field of a curve  $X$ , and a minimal reverse-reading automaton that generates  $\mathbf{a}$  embeds into the differentials of  $X$  in a natural way. This brings to bear the machinery of algebraic curves, and in particular the Riemann–Roch theorem. This idea was introduced by David Speyer [\[2010\]](#) and used to give a new proof of the “algebraic implies automatic” direction of Christol’s theorem. Building on Speyer’s work, we improve the complexity bound implicit in his proof.

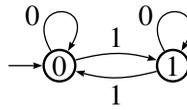
The paper is organized as follows. [Section 2](#) reviews the theory of finite automata and automatic sequences. [Section 3](#) introduces the connection with algebraic geometry, leading to the proof of [Theorem 1.2](#). We also discuss the problem of state complexity growth as the field varies: if  $K$  is a number field and  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in K[[x]]$  is algebraic over  $K(x)$ , then the state complexity of the reduced sequences  $\mathbf{a}_p$  varies with the prime  $p$  in a way controlled by the algebraic nature of  $y$ . [Section 4](#) illustrates some detailed examples of our method.

## 2. Automata, sequences, and representations

**2A. Finite automata and automatic sequences.** A comprehensive introduction to finite automata and automatic sequences can be found in the book of Allouche and Shallit [\[2003\]](#). We give a brief overview of the theory for the convenience of the reader.

A *finite automaton* or DFAO (*deterministic finite automaton with output*)  $M$  consists of a finite set  $\Sigma$  known as the *input alphabet*, a finite set  $\Delta$  known as the *output alphabet*, a finite set of *states*  $Q$ , a distinguished *initial state*  $q_0 \in Q$ , a *transition function*  $\delta : Q \times \Sigma \rightarrow Q$ , and an *output function*  $\tau : Q \rightarrow \Delta$ .

Let  $\Sigma^*$  (the *Kleene closure* of  $\Sigma$ ) be the monoid of all finite-length words over  $\Sigma$  under the operation of juxtaposition, including an empty word as the identity element. The function  $\delta$  can be prolonged to a function  $\delta : Q \times \Sigma^* \rightarrow Q$  by inductively defining  $\delta(q_i, wa) = \delta(\delta(q_i, w), a)$  for  $w \in \Sigma^*$  and  $a \in \Sigma$ . Therefore a DFAO  $M$  induces a map  $f_M : \Sigma^* \rightarrow \Delta$  defined by  $f_M(w) = \tau(\delta(q_0, w))$  under the



**Figure 1.** Thue–Morse 2-DFAO  $T$ .

*forward-reading* convention. If we let  $w^R$  denote the reverse of the word  $w$ , then the *reverse-reading* convention is  $f_M(w) = \tau(\delta(q_0, w^R))$ . A function  $f : \Sigma^* \rightarrow \Delta$  is a *finite-state function* if  $f = f_M$  for some DFAO  $M$ . A DFAO is *minimal* if it has the smallest number of states among automata that induce the same function  $f_M$ .

A helpful way of visualizing a DFAO  $M$  is through its *transition diagram*. This is a directed graph with vertex set  $Q$  and directed edges that join  $q$  to  $\delta(q, a)$  for each  $q \in Q$  and  $a \in \Sigma$ . The initial state is marked by an incoming arrow with no source. The states are labeled by their output  $\tau(q)$ . **Figure 1** shows the transition diagram of the Thue–Morse DFAO  $T$  with  $\Sigma = \Delta = \{0, 1\}$ , where  $f_T(w) = 1$  if and only if  $w \in \{0, 1\}^*$  contains an odd number of 1s.

Let  $p \geq 2$  be an integer (not necessarily prime) and let  $(n)_p$  denote the base- $p$  expansion of the integer  $n \geq 0$ . A sequence  $\mathbf{a}$  is  *$p$ -automatic* if there exists a DFAO  $M$  with input alphabet  $\Sigma_p = \{0, 1, \dots, p-1\}$  such that  $\mathbf{a}(n) = f_M((n)_p)$ ; we say that  $M$  *generates*  $\mathbf{a}$ . It is known that a sequence is  $p$ -automatic with respect to the forward-reading convention if and only if it is  $p$ -automatic with respect to the reverse-reading convention [Allouche and Shallit 2003, Theorem 5.2.3]. (We prove a quantitative version of this fact in [Proposition 2.4](#).) A DFAO with input alphabet  $\Sigma_p$  is called a  *$p$ -DFAO*.

Let  $\mathbf{a}$  be a  $p$ -automatic sequence. As in the introduction, the *forward-reading complexity*  $N_p^f(\mathbf{a})$  is the number of states in a minimal forward-reading  $p$ -DFAO that generates  $\mathbf{a}$ , and the *reverse-reading complexity*  $N_p(\mathbf{a})$  is the number of states in a minimal reverse-reading  $p$ -DFAO that generates  $\mathbf{a}$ .

**Remark 2.1.** Base- $p$  expansions are only unique if we disallow leading zeros — for example, the binary strings 11 and 011 both represent the integer 3. This creates a minor ambiguity in the minimality of a generating DFAO for a sequence, as it may be the case that a larger DFAO is needed if we require that the same output is produced for *every possible* base- $p$  expansion of an integer (it is not even *a priori* clear that both definitions of “ $p$ -automatic” are equivalent; see [Allouche and Shallit 2003, Theorem 5.2.1]). Throughout this paper we enforce the stricter requirement that the generating DFAO gives the same output regardless of leading zeros. (This is necessary for minimality to translate correctly from automata to curves.)

The canonical example of an automatic sequence is the 2-automatic Thue–Morse sequence

$$\mathbf{a} = 01101001 \dots,$$

where  $\mathbf{a}(n) = f_T((n)_2)$  for the Thue–Morse automaton  $T$ . The term  $\mathbf{a}(n)$  is the parity of the sum of the bits in the binary expansion of  $n$ . Note that  $T$  generates  $\mathbf{a}$  under both the forward-reading and reverse-reading conventions, and  $T$  is obviously minimal, so  $N_2(\mathbf{a}) = N_2^f(\mathbf{a}) = 2$ .

There are many characterizations of a sequence that are equivalent to being  $p$ -automatic. We mention two, which are relevant to computing state complexity. The first is due to Eilenberg and relies on the notion of the  $p$ -kernel of  $\mathbf{a}$ , which is defined to be the set of sequences  $n \mapsto \mathbf{a}(p^i n + j)$  for all  $i \geq 0$  and  $0 \leq j \leq p^i - 1$ . The second actually holds in more generality than automatic sequences: it is an easy adaptation of the Myhill–Nerode theorem to the DFAO model.

**Theorem 2.2** (Eilenberg). *For  $p \geq 2$ , the  $p$ -kernel of  $\mathbf{a}$  is finite if and only if  $\mathbf{a}$  is  $p$ -automatic. Moreover,  $N_p(\mathbf{a})$  is precisely the size of the  $p$ -kernel of  $\mathbf{a}$ .*

*Proof.* See [Eilenberg 1974, Proposition V.3.3] or [Allouche and Shallit 2003, Proposition 6.6.2]. See [Derksen 2007, Proposition 4.9] for the claim of minimality (this minimality is in the strict sense of Remark 2.1, as a smaller DFAO may exist otherwise).  $\square$

Let  $f : \Sigma^* \rightarrow \Delta$  be any function. For  $x, y \in \Sigma^*$ , define  $x \sim y$  to mean  $f(xz) = f(yz)$  for all  $z \in \Sigma^*$ . Then  $\sim$  is an equivalence relation on  $\Sigma^*$ , called the Myhill–Nerode equivalence relation.

**Theorem 2.3** (Myhill–Nerode). *The equivalence relation  $\sim$  has finitely many equivalence classes if and only if  $f$  is a finite-state function. The number of equivalence classes of  $\sim$  is the minimal number of states in a forward-reading DFAO  $M$  such that  $f = f_M$ .*

*Proof.* See [Allouche and Shallit 2003, Theorem 4.1.8 and p. 149].  $\square$

**2B. Automata from  $p$ -representations.** Another way of characterizing  $p$ -automatic sequences is by  $p$ -representations. Let  $\mathbf{a}$  be a sequence taking values in a field  $k$ . A  $p$ -representation of  $\mathbf{a}$  consists of a finite-dimensional vector space  $V$  over  $k$ , a vector  $v \in V$ , a morphism of monoids  $\phi : \Sigma_p^* \rightarrow \text{End}(V)$ , and a linear functional  $\lambda \in V^* = \text{Hom}(V, k)$ , such that for any positive integer  $n$ ,

$$\mathbf{a}(n) = \lambda \phi((n)_p) v.$$

A sequence that admits a  $p$ -representation is known as  $p$ -regular [Allouche and Shallit 2003, Chapter 16]. Equivalently, its associated power series is *recognizable* in the language of [Berstel and Reutenauer 1988] (see also [Salomaa and Soittola 1978]).

We also make the nonstandard but natural definition of a  $p$ -antirepresentation of  $\mathbf{a}$ , which consists of the data of a representation except that  $\phi : \Sigma_p^* \rightarrow \text{End}(V)$  is an antimorphism of monoids, that is,  $\phi(wv) = \phi(v)\phi(w)$ . Antirepresentations on  $V$  correspond to representations on the dual space  $V^*$ . In Proposition 2.4 we show that

when  $k$  is finite of characteristic  $p$ ,  $p$ -representations give rise to reverse-reading automata and  $p$ -antirepresentations give rise to forward-reading automata.

An obvious necessary condition for a sequence to be automatic is that it assumes finitely many values. It is not hard to show that a sequence over a field is  $p$ -automatic if and only if it is both  $p$ -regular and assumes finitely many values (see [Allouche and Shallit 2003, Theorem 16.1.5] or [Berstel and Reutenauer 1988, Theorem V.2.2]). We give a quantitative proof of this fact when  $k$  is a finite field, in which case the “finitely many values” hypothesis holds trivially. Our argument will allow us to deduce a bound on state complexity.

**Proposition 2.4.** *Let  $p$  be a prime or prime power and let  $k = \mathbb{F}_p$ . The sequence  $\mathbf{a}$  over  $k$  is  $p$ -regular if and only if it is  $p$ -automatic. Furthermore, if  $\mathbf{a}$  has a  $p$ -representation on a vector space  $V$  of dimension  $m$ , then  $N_p^f(\mathbf{a})$  and  $N_p(\mathbf{a})$  are both at most  $p^m$ .*

*Proof.* First assume that  $\mathbf{a}$  is  $p$ -automatic. There exists a reverse-reading  $p$ -DFAO  $M$  such that  $f_M((n)_p^R) = \mathbf{a}(n)$ . We construct a representation for  $\mathbf{a}$  analogous to the regular representation in group theory. Let  $q_1, \dots, q_m$  be the states of  $M$  and let  $V = k^m$ . Let  $v = e_1$ , the first standard basis vector of  $V$ . For  $i \in \Sigma_p$ , define the matrix  $\phi(i) \in k^{m \times m} \simeq \text{End}(V)$  by

$$\phi(i)_{a,b} = \begin{cases} 1 & \text{if } \delta_i(q_b) = q_a, \\ 0 & \text{otherwise,} \end{cases}$$

and extend  $\phi$  to a morphism from  $\Sigma_p^*$  to  $k^{m \times m}$ . Let  $\lambda$  be defined by  $\lambda(e_j) = \tau(q_j)$  for each  $j$  and extended linearly to a functional  $\lambda : V \rightarrow k$ . This defines a  $p$ -representation of  $\mathbf{a}$ , which can be pictured as embedding the states of  $M$  into  $V$  and realizing the transition function as a set of  $p$  linear transformations.

Now assume instead that  $\mathbf{a}$  is  $p$ -regular. Let  $(V, v, \phi, \lambda)$  be a  $p$ -representation of  $\mathbf{a}$  with  $\dim V = m$ . We construct a reverse-reading DFAO  $M$  as follows. The initial state  $q_0$  is  $v$ , the set of states is  $Q = \{\phi(w)v : w \in \Sigma_p^*\}$ , the transition function is given by  $\delta(w, i) = \phi(i)(w)$ , and the output function is  $\tau(w) = \lambda(w)$ . It is a matter of unraveling notation to see that  $M$  outputs the sequence  $\mathbf{a}$ , and  $M$  has at most  $|V| = p^m$  states.

We now construct a  $p$ -antirepresentation for the sequence  $\mathbf{a}$ . Let  $\phi^T : \Sigma_p^* \rightarrow \text{End}(V^*)$  be the antimorphism defined by  $\phi^T(w) = \phi(w)^T$ , where  $T$  denotes transpose. Now  $(V^*, \lambda, \phi^T, v)$  is a  $p$ -antirepresentation of  $\mathbf{a}$ , where we identify  $V$  with  $(V^*)^*$  in the natural way. If  $(n)_p = c_u \cdots c_1 c_0$ , then

$$\mathbf{a}(n) = \lambda\phi((n)_p)v = \lambda\phi(c_u) \cdots \phi(c_0)v,$$

so thinking of  $v$  as an element of  $(V^*)^*$ , we have

$$\mathbf{a}(n) = v(\lambda\phi(c_u) \cdots \phi(c_0)) = v\phi^T(c_0) \cdots \phi^T(c_u)\lambda = v\phi^T(c_u \cdots c_0)\lambda = v\phi^T((n)_p)\lambda.$$

This corresponds to a forward-reading DFAO  $M$  in the following way: let the initial state  $q_0$  of  $M$  be  $\lambda$ , the set of states be  $Q = \{\phi^T(w)\lambda : w \in \Sigma_p^*\}$ , the transition function be  $\delta(\mu, i) = \phi^T(i)(\mu)$ , and the output function be  $\tau(\mu) = v^T(\mu) = \mu(v)$ . Taking transposes has the effect of reversing input words, so this gives a forward-reading DFAO that outputs the sequence  $\mathbf{a}$ , and it has at most  $p^m$  states, as  $\dim V = \dim V^*$ .  $\square$

**Remark 2.5.** A special case of the antirepresentation constructed in [Proposition 2.4](#) gives a standard result of automata theory; if  $\Delta = \{0, 1\}$ , so that  $M$  either accepts or rejects each input string, and  $M$  has  $n$  states, then a minimal reversed automaton for  $M$  has at most  $2^n$  states. We can identify  $\Delta$  with  $\mathbb{F}_2$ , and the regular representation is on the vector space  $\mathbb{F}_2^n$ .

The representation constructed in [Proposition 2.4](#) produces a  $p$ -DFAO where the states are identified with a subset of  $V$  and the transitions are realized as linear transformations. In general, this is not a minimal DFAO. Much of our work in the rest of the paper will be describing canonical representations that produce minimal DFAO.

Somewhat surprisingly, for any  $p$ -representation of  $\mathbf{a}$ , the forward-reading  $p$ -DFAO antirepresentation in [Proposition 2.4](#) is minimal as long as  $V$  equals the linear span of  $\{\phi(w)v : w \in \Sigma_p^*\}$ . This assumption on  $V$  loses no generality, because we can always replace  $V$  with this subspace (in particular, satisfying this assumption does *not* mean the corresponding reverse-reading automaton is minimal). This observation is to our knowledge new, and we prove it in [Proposition 2.6](#). In a sense, this is an analogue via representations of the minimization algorithm of Brzozowski [[Brzozowski 1963](#); [Shallit 2009](#)].

**Proposition 2.6.** *Let  $\mathbf{a}$  be a sequence taking values in a finite field  $k$ , and let  $(V, v, \phi, \lambda)$  be a  $p$ -representation of  $\mathbf{a}$ . Assume without loss of generality that  $V$  is the  $k$ -linear span of  $\{\phi(w)v : w \in \Sigma_p^*\}$ . The DFAO  $M$  corresponding to the antirepresentation in [Proposition 2.4](#) is a minimal forward-reading  $p$ -DFAO that generates  $\mathbf{a}$ .*

*Proof.* The state set of  $M$  is  $Q = \{\phi^T(w)\lambda : w \in \Sigma_p^*\}$  with initial state  $\lambda$ , the transition function is  $\delta(\mu, i) = \phi(i)^T(\mu)$ , and the output function is  $\tau(\mu) = \mu(v)$  for some fixed  $v \in V$ . We show that the states of  $Q$  are in one-to-one correspondence with the Myhill–Nerode equivalence classes of the finite-state function  $f_M$  as in [Theorem 2.3](#).

Let  $[x]$  be the equivalence class of  $x \in \Sigma_p^*$ . We need to show that  $[x] = [y]$  if and only if  $\phi^T(x)(\lambda) = \phi^T(y)(\lambda)$ . We have

$$[x] = \{y \in \Sigma_p^* : \tau(\phi^T(xz)\lambda) = \tau(\phi^T(yz)\lambda) \text{ for all } z \in \Sigma_p^*\},$$

and the computation  $\tau(\phi^T(xz)\lambda) = \tau(\lambda\phi(xz)) = \lambda\phi(x)\phi(z)v$  shows that

$$\begin{aligned} [x] &= \{y \in \Sigma_p^* : \lambda\phi(x)\phi(z)v = \lambda\phi(y)\phi(z)v \text{ for all } z \in \Sigma_p^*\} \\ &= \{y \in \Sigma_p^* : \lambda\phi(x) = \lambda\phi(y) \text{ in } V^*\}, \end{aligned}$$

because  $V$  is the span of the set  $\{\phi(z)v : z \in \Sigma_p^*\}$ . So  $[x]$  is the precisely the set of all  $y$  such that  $\phi^T(x)\lambda = \phi^T(y)\lambda$ . By the Myhill–Nerode theorem,  $M$  is a minimal forward-reading DFAO that generates  $\mathbf{a}$ . □

**2C. Power series and bounds on degree and height.** We develop some standard machinery that is used in the proof of Christol’s theorem. Let  $k$  be a perfect field of characteristic  $p$ , for example, a finite field  $\mathbb{F}_{p^r}$ . Let

$$y = \sum_{n=-\infty}^{\infty} \mathbf{a}(n)x^n \in k((x)),$$

where  $\mathbf{a}(n) = 0$  for all sufficiently large negative  $n$ . Define

$$\Lambda_i(y) = \sum_{n=-\infty}^{\infty} \mathbf{a}(pn + i)^{1/p}x^n. \tag{2.7}$$

The operators  $\Lambda_i$  are  $\mathbb{F}_p$ -linear (not necessarily  $k$ -linear) endomorphisms of the field  $k((x))$ . They are known in this context as Cartier operators. Observe that

$$\begin{aligned} y &= \sum_{i=0}^{p-1} \sum_{n=-\infty}^{\infty} \mathbf{a}(pn + i)x^{pn+i} \\ &= \sum_{i=0}^{p-1} x^i \sum_{n=-\infty}^{\infty} \mathbf{a}(pn + i)x^{pn} \\ &= \sum_{i=0}^{p-1} x^i \left( \sum_{n=-\infty}^{\infty} \mathbf{a}(pn + i)^{1/p}x^n \right)^p \end{aligned} \tag{2.8}$$

and therefore

$$y = \sum_{i=0}^{p-1} x^i (\Lambda_i(y))^p. \tag{2.9}$$

If  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_p[[x]]$ , it is easy to see that the  $p$ -kernel of  $\mathbf{a}$  is in bijection with the orbit of  $y$  under the monoid generated by the  $\Lambda_i$  operators, as taking  $p$ -th roots fixes each element of  $\mathbb{F}_p$ . If  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$  for  $q = p^r$ , then applying  $r$ -fold compositions of the  $\Lambda_i$  operators gives  $q$ -ary decimations of the sequence  $\mathbf{a}$ . That is, if

$$c = i_r p^{r-1} + i_{r-1} p^{r-2} + \dots + i_2 p + i_1,$$

where each  $i_j \in \{0, \dots, p-1\}$ , then

$$\begin{aligned} \Lambda_{i_1} \Lambda_{i_2} \cdots \Lambda_{i_r}(y) &= \sum_{n=0}^{\infty} \mathbf{a}(p^r n + i_r p^{r-1} + \cdots + i_2 p + i_1)^{1/p^r} x^n \\ &= \sum_{n=0}^{\infty} \mathbf{a}(qn + c)x^n, \end{aligned} \quad (2.10)$$

because  $\mathbb{F}_q$  is fixed under taking  $q$ -th roots. It follows that

$$y = \sum_{0 \leq i_1, \dots, i_r \leq p-1} x^{i_r p^{r-1} + \cdots + i_2 p + i_1} (\Lambda_{i_1} \Lambda_{i_2} \cdots \Lambda_{i_r}(y))^q. \quad (2.11)$$

**Remark 2.12.** The operators  $\Lambda_i$  are usually defined by  $\Lambda_i(y) = \sum_{n=-\infty}^{\infty} \mathbf{a}(qn+i)x^n$  when  $k = \mathbb{F}_q$ ; see for example [Adamczewski and Bell 2012; 2013; Allouche and Shallit 2003]. With this definition, (2.11) takes on the much simpler form

$$y = \sum_{i=0}^{q-1} x^i (\Lambda_i(y))^q.$$

However, our definition fits more naturally into the geometric setting of Section 3 because it is invariant under base extension, whereas the usual definition depends on a choice of  $\mathbb{F}_q$  fixed in advance.

Continue to assume that  $y \in \mathbb{F}_q[[x]]$ , where  $p$  is prime and  $q = p^r$ . Define  $S_q$  to be the monoid generated by all  $r$ -fold compositions of the  $\Lambda_i$  operators. The  $q$ -kernel of  $\mathbf{a}$  is in bijection with the orbit of  $y$  under  $S_q$ , which we denote  $S_q(y)$ . If  $\mathbf{a}$  is a  $q$ -automatic sequence, then by Eilenberg's Theorem  $S_q(y)$  is finite and  $|S_q(y)| = N_q(\mathbf{a})$ . Moreover, we have a  $q$ -representation for  $\mathbf{a}$ :  $V$  is the finite-dimensional  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_q[[x]]$  spanned by the power series whose coefficient sequences are in the  $q$ -kernel of  $\mathbf{a}$ ,  $\phi$  is defined so that, for  $i \in S_q$ ,  $\phi(i)$  maps  $\sum_{n=0}^{\infty} \mathbf{a}(n)x^n$  to  $\sum_{n=0}^{\infty} \mathbf{a}(qn+i)x^n$  by the  $r$ -fold composition of the  $\Lambda_i$  operators given in (2.11), and the linear functional  $\lambda$  maps a power series to its constant term.

The standard proof of the ‘‘algebraic implies automatic’’ half of Christol's theorem [Christol et al. 1980; Christol 1979; Allouche and Shallit 2003, Theorem 12.2.5] follows from the observation that  $y$  is algebraic if and only if it lies in a finite-dimensional  $\mathbb{F}_q$ -subspace of  $\mathbb{F}_q((x))$  invariant under  $S_q$ . Given an algebraic power series  $y$ , it is easy to construct an invariant space using Ore's lemma [Allouche and Shallit 2003, pp. 355–356], which leads to the prior bounds on state complexity mentioned in the introduction, but the dimension of the space constructed is often far larger than the dimension of the linear span of  $S_q(y)$ . We achieve a sharper bound on the dimension by introducing some relevant machinery from algebraic geometry in the next section. First we demonstrate some easy upper bounds on

height and degree in terms of reverse-reading state complexity that can be extracted from the usual proof of Christol’s theorem.

**Proposition 2.13.** *Let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$ . Assume  $\mathbf{a}$  is  $q$ -automatic and  $N_q(\mathbf{a}) = m$ . Then  $y$  is algebraic,  $\deg y \leq q^m - 1$ , and  $h(y) \leq mq^{m+1}$ .*

*Proof.* Let  $S_q(y) = \{y_1, \dots, y_m\}$ . From (2.11), for each  $i \in \{1, \dots, m\}$  we have

$$y_i \in \langle y_1^q, \dots, y_m^q \rangle,$$

where the angle brackets  $\langle \dots \rangle$  indicate  $\mathbb{F}_q(x)$ -linear span. So

$$y_i^q \in \langle y_1^{q^2}, \dots, y_m^{q^2} \rangle,$$

and eventually

$$y_i^{q^m} \in \langle y_1^{q^{m+1}}, \dots, y_m^{q^{m+1}} \rangle.$$

Therefore

$$\{y_i, y_i^q, y_i^{q^2}, \dots, y_i^{q^m}\} \subseteq \langle y_1^{q^{m+1}}, \dots, y_m^{q^{m+1}} \rangle,$$

which forces an  $\mathbb{F}_q(x)$ -linear relation among  $y_i, y_i^q, y_i^{q^2}, \dots, y_i^{q^m}$ , that is, an algebraic equation satisfied by  $y_i$ . In particular,  $y$  is algebraic, which proves the “automatic implies algebraic” direction of Christol’s theorem. If  $y \neq 0$  we can cancel  $y$  to deduce  $\deg y \leq q^m - 1$  (if  $y = 0$  this is trivially true).

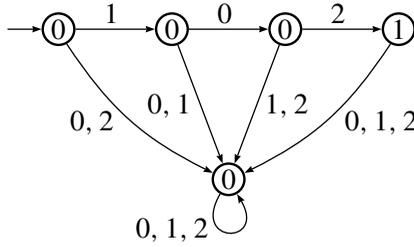
Working through the chain of linear dependences shows that each  $y_i^{q^k}$  can be written as a linear combination of  $\{y_1^{q^{m+1}}, \dots, y_m^{q^{m+1}}\}$  with polynomial coefficients of degree at most  $q^{m+1}$ . A standard argument in linear algebra shows that there is a vanishing linear combination of  $\{y_i, y_i^q, \dots, y_i^{q^m}\}$  with polynomial coefficients of degree at most  $mq^{m+1}$ .  $\square$

It is easy to construct infinite families of power series for which degree and height grow exponentially in  $N_q(\mathbf{a})$ , which we do in Examples 2.14 and 2.15. It is not clear whether the bounds of Proposition 2.13 are sharper than these families indicate.

**Example 2.14.** Let  $y = x^n$  and let  $\mathbf{a}$  be the sequence with a 1 in the  $n$ -th position and 0 in every other position. We have  $N_q(\mathbf{a}) = \lceil \log_q(n) \rceil + 1$ , because a  $q$ -DFAO generating  $\mathbf{a}$  needs  $\lceil \log_q(n) \rceil$  states to recognize the base- $q$  expansion of  $n$  and one additional “trap state” that outputs zero on any input that deviates from this expansion. So  $h(y)$  grows exponentially in the number of states required. For example, Figure 2 gives a 3-DFAO that outputs 1 on the word 201 and 0 otherwise.

**Example 2.15.** The degree bound of Proposition 2.13 is nearly sharp for those degrees that are powers of  $q$ . We argue that the unique solution in  $\mathbb{F}_q[[x]]$  to the Artin–Schreier equation

$$y^{q^m} - y = x,$$



**Figure 2.** Minimal 3-DFAO that outputs 1 on 201 and 0 otherwise.

which is

$$y = x + x^{q^m} + x^{q^{2m}} + x^{q^{3m}} + \dots,$$

satisfies  $N_q(\mathbf{a}) = m + 2$ , so  $\deg y = q^{N_q(\mathbf{a})-2}$ . As usual, we identify the states of a reverse-reading  $q$ -automaton that outputs  $\mathbf{a}$  with the orbit of  $y$  under  $S_q$ . We compute

$$\phi(0)(y) = \sum_{n=0}^{\infty} \mathbf{a}(qn)x^n = x^{q^{m-1}} + x^{q^{2m-1}} + x^{q^{3m-1}} + \dots,$$

$$\phi(1)(y) = \sum_{n=0}^{\infty} \mathbf{a}(qn+1)x^n = 1,$$

$$\phi(c)(y) = \sum_{n=0}^{\infty} \mathbf{a}(qn+c)x^n = 0,$$

for  $2 \leq c \leq q-1$ . It is clear that  $S_q(1) = \{0, 1\}$ , and

$$\phi(0)^2(y) = x^{q^{m-2}} + x^{q^{2m-2}} + x^{q^{3m-2}} + \dots,$$

$$\phi(0)^3(y) = x^{q^{m-3}} + x^{q^{2m-3}} + x^{q^{3m-3}} + \dots,$$

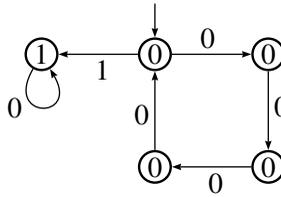
⋮

$$\phi(0)^{m-1}(y) = x^q + x^{q^{m+1}} + x^{q^{2m+1}} + \dots,$$

$$\phi(0)^m(y) = x + x^{q^m} + x^{q^{2m}} + \dots = y.$$

Except for  $y$ , the power series in this list are all  $q$ -th powers, so any element of  $S_q$  that includes a  $\Lambda_i$  operator other than  $\Lambda_0$  sends each one to zero. By Eilenberg's theorem, a minimal reverse-reading automaton that outputs  $\mathbf{a}$  has  $m+2$  states. Figure 3 depicts such an automaton for  $m=4$ . Any undrawn transition arrow leads to a trap state  $q_T$  (not pictured) where  $\delta(q_T, i) = q_T$  for every  $i \in \Sigma_q$  and  $\tau(q_T) = 0$ .

A sequence is  $p$ -automatic if and only if it is  $p^r$ -automatic for any  $r \geq 1$  [Allouche and Shallit 2003, Theorem 6.6.4], so it makes sense to discuss the base- $p$  state complexity of  $\mathbf{a}$ , as well as the base- $q$  state complexity. In fact, Christol's theorem is usually stated in the equivalent form that for any  $r \geq 1$ , a power series over  $\mathbb{F}_{p^r}$  is



**Figure 3.** Minimal  $q$ -DFAO generating the coefficients of  $y$ , where  $y^{q^4} - y = x$ .

algebraic if and only if its coefficient sequence is  $p$ -automatic. The next proposition shows that, for a given  $q$  and  $p$ , there is no qualitative difference between base- $p$  and base- $q$  complexity, in the sense they are at most a multiplicative constant apart.

**Proposition 2.16.** *Let  $\mathbf{a}$  be  $p$ -automatic and  $q = p^r$ . Then*

$$N_q(\mathbf{a}) \leq N_p(\mathbf{a}) \leq \frac{q-1}{p-1} N_q(\mathbf{a}) \quad \text{and} \quad N_q^f(\mathbf{a}) \leq N_p^f(\mathbf{a}) \leq \frac{q-1}{p-1} N_q^f(\mathbf{a}).$$

*Proof.* First we handle reverse-reading complexity. Without loss of generality, assume that the output alphabet  $\Delta$  of the DFAO that produces  $\mathbf{a}$  is a subset of  $\mathbb{F}_{p^N}$  for some  $N$  with  $\mathbb{F}_q \subseteq \mathbb{F}_{p^N}$ . The lower bound on  $N_p(\mathbf{a})$  is clear from the fact that  $S_q(y) \subseteq S_p(y)$  for  $y = \sum \mathbf{a}(n)x^n$ .

For the upper bound, let  $M_p$  be a minimal reverse-reading  $p$ -DFAO that outputs  $\mathbf{a}$ . Observe that  $M_p$  contains the  $q$ -DFAO  $M_q$  (which also outputs  $\mathbf{a}$ ) as a “subDFAO”, where the transitions in  $M_q$  are achieved by following  $r$ -fold transitions inside  $M_p$ . So the states of  $M_p$  that are not in  $M_q$  comprise at most one  $p$ -ary tree of height  $r$  rooted at each state of  $M_q$ . So

$$N_p(\mathbf{a}) \leq (1 + p + p^2 + \dots + p^{r-1})|M_q| = \frac{p^r - 1}{p - 1} N_q(\mathbf{a}),$$

which yields the claimed inequality.

To pass to forward-reading state complexity, follow the dualizing construction of Proposition 2.4 to embed the states of a forward-reading  $p$ -DFAO in some vector space over  $\mathbb{F}_{p^N}$ . Then let  $S_p^T$  and  $S_q^T$  be monoids consisting of the transposes of the operators in  $S_p$  and  $S_q$ . The same arguments as above now apply.  $\square$

### 3. Curves, the Cartier operator, and Christol’s theorem

**3A. Curves and the Cartier operator.** At this point we recall some standard definitions and terminology from the algebraic geometry of curves. For an introduction to the subject, see [Hartshorne 1977, Chapter IV; Silverman 2009, Chapter II; Stichtenoth 2009].

Let  $k$  be a perfect field of characteristic  $p$  and let  $X/k$  be a smooth projective algebraic curve. Denote the function field  $k(X)$  by  $K$ . Let  $\Omega = \Omega_{K/k}$  be the  $K$ -vector space of (Kähler) differentials of  $K/k$ , which is one-dimensional.

Let  $P$  be a (closed) point of  $X$ , or equivalently a place of  $K$ . (Whenever we refer to points of  $X$ , we will always mean closed points.) Write  $v_P(f)$  or  $v_P(\omega)$  for the valuation given by the order of vanishing of  $f \in K^\times$  or  $\omega \in \Omega \setminus \{0\}$  at  $P$ . The valuation ring  $\mathcal{O}_P$  is defined to be

$$\mathcal{O}_P = \{f \in K^\times : v_P(f) \geq 0\} \cup \{0\},$$

with maximal ideal

$$\mathfrak{m}_P = \{f \in K^\times : v_P(f) \geq 1\} \cup \{0\}.$$

The degree  $\deg P$  is  $\dim_k \mathcal{O}_P/\mathfrak{m}_P$ . Write  $\text{res}_P(\omega)$  for the residue of  $\omega$  at  $P$ .

Let  $\text{Div}_k(X)$  denote the group of  $k$ -rational divisors of  $X$ . If  $f \in K^\times$ , define

$$\begin{aligned} (f)_0 &= \sum_{v_P(f) > 0} v_P(f)P, \\ (f)_\infty &= \sum_{v_P(f) < 0} -v_P(f)P, \\ (f) &= (f)_0 - (f)_\infty. \end{aligned}$$

For  $D = \sum_P n_P P \in \text{Div}_k(X)$ , write  $D \geq 0$  if  $D$  is effective, that is, if  $n_P \geq 0$  for all  $P$ . Define

$$\mathcal{L}(D) = \{f \in K^\times : (f) + D \geq 0\} \cup \{0\} \quad \text{and} \quad \Omega(D) = \{\omega \in \Omega \setminus \{0\} : (\omega) + D \geq 0\} \cup \{0\}.$$

By the Riemann–Roch theorem,

$$\dim_k \Omega(D) = \dim_k \mathcal{L}(-D) + \deg D + g - 1.$$

If  $D$  is effective, then  $\mathcal{L}(-D) = \{0\}$  and

$$\dim_k \Omega(D) = \deg D + g - 1.$$

For an effective divisor  $D$ , it will be convenient to introduce the nonstandard notation  $\sqrt{D}$  for the “radical” of  $D$ , that is,

$$\sqrt{D} = \sum_{v_P(D) > 0} P.$$

Let  $x \in K$  be a separating variable ( $x \notin K^p$ , equivalently  $dx \neq 0$ ). For such an  $x$ , there is some point  $P$  of  $X$  such that  $v_P(x)$  is not divisible by  $p$ . By an easy argument using valuations at  $P$ , the powers  $1, x, x^2, \dots, x^{p-1}$  are linearly independent over  $K^p$ . As  $[K : K^p] = p$  by standard facts about purely inseparable

extensions [Stichtenoth 2009, Proposition 3.10.2], the set  $\{1, x, \dots, x^{p-1}\}$  forms a basis of  $K$  over  $K^p$ . Thus, any  $\omega \in \Omega$  can be written as

$$\omega = (u_0^p + u_1^p x + \dots + u_{p-1}^p x^{p-1}) dx, \quad (3.1)$$

for unique  $u_0, \dots, u_{p-1} \in K$ . Define a map  $\mathcal{C} : \Omega \rightarrow \Omega$  by

$$\mathcal{C}(\omega) = u_{p-1} dx. \quad (3.2)$$

It is true, but far from obvious, that  $\mathcal{C}$  does not depend on the choice of  $x$  [Stichtenoth 2009, p. 183]. The operator  $\mathcal{C}$  is an  $\mathbb{F}_p$ -linear endomorphism of  $\Omega$  known as the Cartier operator. This operator is of great importance in characteristic- $p$  algebraic geometry. It can be extended in a natural way to  $r$ -forms of higher-dimensional varieties for any  $r$ , though we do not need this for our purposes (see for example [Cartier 1957; Serre 1958]).

It follows from the definition of  $\mathcal{C}$  that for any  $\omega \in \Omega$ ,

$$\omega = \sum_{i=0}^{p-1} x^i \left( \frac{\mathcal{C}(x^{p-1-i} \omega)}{dx} \right)^p dx. \quad (3.3)$$

Comparing equations (2.9) and (3.3) motivates the following definition. For  $i \in \{0, 1, \dots, p-1\}$ , define the *twisted Cartier operator*  $\sigma_i : \Omega \rightarrow \Omega$  by

$$\sigma_i(\omega) = \mathcal{C}(x^{p-1-i} \omega). \quad (3.4)$$

For this to make sense in an arbitrary function field  $K$ , we need to fix a distinguished separating  $x \in K$  in advance (equivalently, a distinguished separable cover  $X \rightarrow \mathbb{P}^1$ ). Having done so, if  $y \in k((x)) \cap K$ , it is clear that

$$\sigma_i(y dx) = \Lambda_i(y) dx, \quad (3.5)$$

so the  $\sigma_i$  act on differentials just as the  $\Lambda_i$  act on series.

**Remark 3.6.** Equation (3.5) is true in the differential module of any function field  $K$  that contains the Laurent series  $y$ , as long as  $x \in K$  is separating. In particular, we can take  $K = k(x)[y]$ , as the Laurent series field  $k((x))$  is a separable extension of  $k(x)$ . This proves that if  $y$  is algebraic, then the operators  $\Lambda_i$  map  $k(x)[y]$  into itself. This is not at all obvious from the definition of  $\Lambda_i$  as an operator on formal Laurent series.

We summarize some important properties of  $\mathcal{C}$  in the next proposition. These are standard (see e.g., [Stichtenoth 2009, p. 182]), but we sketch proofs for the convenience of the reader.

**Proposition 3.7.** For any  $\omega, \omega' \in \Omega$ ,  $f \in K$ , and any point  $P$  of  $X$ :

$$(1) \mathcal{C}(\omega + \omega') = \mathcal{C}(\omega) + \mathcal{C}(\omega').$$

- (2)  $\mathcal{C}(f^p \omega) = f \mathcal{C}(\omega)$ .
- (3)  $\mathcal{C}(\omega) = 0$  if and only if  $\omega = dg$  for some  $g \in K$ .
- (4) If  $\omega$  is regular at  $P$ , then so is  $\mathcal{C}(\omega)$ .
- (5) If  $\omega$  has a pole at  $P$ , then  $v_P(\mathcal{C}(\omega)) \geq (v_P(\omega) + 1)/p - 1$ , and equality holds if the RHS is an integer. In particular, if  $v_P(\omega) = -1$ , then  $v_P(\mathcal{C}(\omega)) = -1$ .
- (6) If  $\deg P = 1$ , then  $\text{res}_P(\mathcal{C}(\omega))^p = \text{res}_P(\omega)$ .

*Proof.* Statements (1) and (2) are immediate from the definition and imply that  $\mathcal{C}$  is  $\mathbb{F}_p$ -linear.

Statement (3) follows from the fact that there is no  $g \in K$  such that  $dg = x^{p-1} dx$ . If there were such a  $g$ , we would have  $dg/dx = x^{p-1}$ , but this is impossible because the derivative of  $x^p$  is zero. For the converse, if  $u_{p-1} = 0$ , set

$$g = u_0^p x + u_1^p \frac{x^2}{2} + \cdots + u_{p-2}^p \frac{x^{p-1}}{p-1},$$

and note that no denominator is zero. Then  $\omega = dg$ .

For statement (4), choose a uniformizer  $t$  at  $P$ , which is necessarily separating (if  $t$  is a  $p$ -th power, then  $v_P(t)$  is a multiple of  $p$  and  $t$  cannot be a uniformizer at  $P$ ). Let  $\omega = f dt$ . If  $\omega$  is regular at  $P$ , then so is  $f$ , because  $v_P(dt) = 0$ . So,  $f$  can be written as a power series in  $t$  and  $\mathcal{C}(\omega) = \Lambda_{p-1}(f) dt$ . The series  $\Lambda_{p-1}(f)$  is regular at  $P$ , so  $\mathcal{C}(\omega)$  is also. Statements (5) and (6) follow similarly by writing  $f$  as a Laurent series in  $t$ .  $\square$

**3B. Christol's theorem and complexity bounds.** At this point we fix a prime  $p$  and a prime power  $q = p^r$ . Let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$  be algebraic of degree  $d$ , height  $h$ , and genus  $g$ . Let  $X$  be the normalization of the projective closure of the affine curve defined by the minimal polynomial of  $y$  (after clearing denominators). Set  $K = \mathbb{F}_q(X)$  and  $\Omega = \Omega_{K/\mathbb{F}_q}$ .

Define  $\mathcal{S}_q$  to be the monoid generated by all  $r$ -fold compositions of the operators  $\{\sigma_0, \dots, \sigma_{p-1}\}$ . In particular,  $\mathcal{S}_p = \langle \sigma_0, \dots, \sigma_{p-1} \rangle$ . We write  $\mathcal{S}_q(\omega)$  for the orbit of  $\omega$  under  $\mathcal{S}_q$ . Note that  $dx \neq 0$  because  $\mathbb{F}_q(x) \subseteq K \subseteq \mathbb{F}_q((x))$ , so  $K/\mathbb{F}_q(x)$  is separable (the Laurent series field is a separable extension of the rational function field). Therefore (3.5) holds, so the orbits  $\mathcal{S}_q(y dx)$  and  $\mathcal{S}_q(y)$  are in bijection. So if  $\mathcal{S}_q(y dx)$  is finite, then  $\mathbf{a}$  is  $p$ -automatic, and  $|\mathcal{S}_q(y dx)| = N_q(\mathbf{a})$ .

We now present the proof of the ‘‘algebraic implies automatic’’ direction of Christol's theorem due to David Speyer [2010]. As indicated above, the crux of the argument is to show that the orbit  $\mathcal{S}_q(y dx)$  is finite. By Proposition 2.16, it loses essentially nothing to replace  $\mathcal{S}_q(y dx)$  with the larger orbit  $\mathcal{S}_p(y dx)$ .

**Proposition 3.8** (Speyer). *The sequence  $\mathbf{a}$  is  $q$ -automatic.*

*Proof.* Let  $P$  be a point of  $X$ . By [Proposition 3.7](#), if neither  $x$  nor  $\omega$  has a pole at  $P$ , then  $\sigma_i(\omega) = \mathcal{C}(x^{p-i-1}\omega)$  does not have a pole at  $P$  for any  $i \in \{0, \dots, p-1\}$ . Therefore, the only places where elements of  $\mathcal{S}_p(y dx)$  can have poles are the finitely many poles of  $y dx$  and of  $x$ .

Now assume that  $P$  is a pole of  $y dx$  or of  $x$ . Let  $n = v_p(y dx)$  and  $m = v_p(x)$ . Applying the inequality of [Proposition 3.7](#) gives

$$v_p(\sigma_i(y dx)) \geq \frac{n+m(p-1-i)+1}{p} - 1.$$

The pole of largest order that  $\sigma_i(y dx)$  could have at  $P$  occurs when both  $n$  and  $m$  are negative. In this case,

$$v_p(\sigma_i(y dx)) \geq \frac{n}{p} + \frac{m(p-1)}{p} + \frac{1}{p} - 1.$$

Applying the same reasoning again shows that

$$v_p(\sigma_j \sigma_i(y dx)) \geq \frac{n}{p^2} + \frac{m(p-1)}{p^2} + \frac{m(p-1)}{p} + \frac{1}{p^2} - 1,$$

and applying it  $k$  times shows that

$$\begin{aligned} v_p(\sigma_{i_k} \cdots \sigma_{i_1}(y dx)) &\geq \frac{n}{p^k} + m(p-1) \left( \frac{1}{p^k} + \frac{1}{p^{k-1}} + \cdots + \frac{1}{p} \right) + \frac{1}{p^k} - 1 \\ &\geq n + \frac{m(p-1)}{p-1} + \frac{1}{p^k} - 1 \\ &> n + m - 1. \end{aligned}$$

Therefore  $v_p(\omega) \geq n + m$  for any  $\omega \in \mathcal{S}_p(y dx)$ . (If one of  $\{n, m\}$  is positive, then it follows in the same way that  $v_p(\omega) \geq \min\{n, m\}$  instead.)

The differentials in  $\mathcal{S}_p(y dx)$  have poles at only finitely many places, and the orders of these poles are bounded. So there is a finite-dimensional  $\mathbb{F}_q$ -vector space that contains  $\mathcal{S}_p(y dx)$ , and in particular  $\mathcal{S}_p(y dx)$  is finite.  $\square$

The Riemann–Roch bound implicit in [Proposition 3.8](#) gives a complexity bound that is a preliminary version of [Theorem 1.2](#). This is [Corollary 3.10](#), for which it will be convenient to use the language of representations. Let  $v = y dx$ , and let  $V$  and  $\lambda$  be as in the setup before [Proposition 3.8](#). Let  $\phi : \Sigma_q^* \rightarrow \text{End}(V)$  be the unique monoid morphism defined for  $c \in \Sigma_q$  by

$$\phi(c) = \sigma_{i_r} \sigma_{i_{r-1}} \cdots \sigma_{i_1},$$

where  $c = i_r p^{r-1} + i_{r-1} p^{r-2} + \cdots + i_2 p + i_1$  with  $0 \leq i_1, \dots, i_r \leq p-1$ . Then by the power series machinery of [Section 2C](#) and the bijection between  $\mathcal{S}_q(y)$  and  $\mathcal{S}_q(y dx)$ , we see that  $(V, v, \phi, \lambda)$  gives a  $q$ -representation of  $\mathbf{a}$ .

**Remark 3.9.** If  $D$  is any divisor such that  $\mathcal{S}_q(y dx) \subseteq \Omega(D)$ , then we can identify  $\lambda$  with an element of  $H^1(X, \mathcal{O}_X(-D))$ . This is because of the natural duality isomorphism

$$H^1(X, \mathcal{O}_X(-D))^* \simeq H^0(X, \Omega_X^1(D)),$$

which is the classical statement of Serre duality for curves [Hartshorne 1977, Chapter III.7]. (The global sections of  $\Omega_X^1(D)$  are exactly what we have called  $\Omega(D)$ .) In fact,  $\lambda$  has an explicit realization as a repartition (adele). See, e.g., [Stichtenoth 2009, Chapter 1.5; Serre 1958, p. 37]. Moreover, the Cartier operator on  $\Omega(D)$  is the transpose (or adjoint) of the Frobenius operator on  $H^1(X, \mathcal{O}_X(-D))$ .

**Corollary 3.10.**  $\max(N_q^f(\mathbf{a}), N_q(\mathbf{a})) \leq q^{h+3d+g-1}$ .

*Proof.* The bounds on the orders of poles in the proof of Proposition 3.8 show that

$$\mathcal{S}_q(y dx) \subseteq \Omega((y dx)_\infty + (x)_\infty),$$

so we may take  $V = \Omega((y dx)_\infty + (x)_\infty)$  in the  $q$ -representation of  $\mathbf{a}$ . By Proposition 2.4, both  $N_q^f(\mathbf{a})$  and  $N_q(\mathbf{a})$  are at most  $|V| = q^{\dim_{\mathbb{F}_q} V}$ . We have

$$\dim_{\mathbb{F}_q} V = \deg((y dx)_\infty + (x)_\infty) + g - 1 \leq \deg(y dx)_\infty + \deg(x)_\infty + g - 1.$$

Let  $\pi_x, \pi_y : X \rightarrow \mathbb{P}^1$  be the projection maps from  $X$  onto the  $x$ - and  $y$ -coordinates. We have  $\deg(x)_\infty = \deg \pi_x = d$  and  $\deg(y)_\infty = \deg \pi_y = h$ . (The easiest way to see this is by looking at the function field inclusions  $\pi_x^* : \mathbb{F}_q(x) \hookrightarrow K$  and  $\pi_y^* : \mathbb{F}_q(y) \hookrightarrow K$ . That is,  $d = [K : \mathbb{F}_q(x)]$  and  $h = [K : \mathbb{F}_q(y)]$ .)

The poles of  $dx$  occur at points which are poles of  $x$ , and the order of a pole of  $dx$  at  $P$  can be at most one more than the order of the pole of  $x$  at  $P$ . So  $\deg(dx)_\infty$  is maximized when the poles of  $x$  are all simple, in which case  $\deg(dx)_\infty = 2 \deg(x)_\infty = 2d$ . The fact that  $\deg(y dx)_\infty \leq \deg(y)_\infty + \deg(dx)_\infty$  gives the upper bound.  $\square$

The bound in Corollary 3.10 is superseded by Theorem 1.2 for large values of  $h$ ,  $d$ , and  $g$ . However, it is simple to prove and is already much better than the previous bounds derived from Ore's Lemma.

We aim to prove Theorem 1.2 by bounding the size of the orbit  $\mathcal{S}_q(y dx)$ . As in the proof of Proposition 3.8, it will be easier to deal with the larger orbit  $\mathcal{S}_p(y dx)$ . By Proposition 2.16, this creates no essential difference in the size of the orbit. To streamline the exposition, we establish some preliminary lemmas. Lemmas 3.11 and 3.12 determine the “eventual behavior” of  $y dx$  under  $\mathcal{S}_p$ . The main difficulty is in handling the orbit of  $y dx$  under the operator  $\sigma_0$  (this is related to the special role that 0 plays in nonuniqueness of base expansions). Recall that  $\sqrt{D}$  is the sum of the points in the support of the divisor  $D$ , neglecting multiplicities.

**Lemma 3.11.** *Let  $V = \Omega((y)_\infty + (x)_\infty + \sqrt{(x)_\infty})$  and  $W = \Omega((y)_\infty + (x)_\infty)$ . Then for any  $i \in \{1, \dots, p-1\}$ ,  $\sigma_i(V) \subseteq W$ , and for any  $i \in \{0, \dots, p-1\}$ ,  $\sigma_i(W) \subseteq W$ .*

*Proof.* Let  $\omega \in V$ . Then for any point  $P$ ,  $v_P(\omega) \geq -v_P((y)_\infty) - 2v_P((x)_\infty)$ . By [Proposition 3.7](#),

$$\begin{aligned} v_p(\sigma_i(y \, dx)) &= v_p(\mathcal{C}(x^{p-1-i} y \, dx)) \\ &\geq \frac{-v_p((y)_\infty) + (-p-1+i)v_p((x)_\infty) + 1}{p} - 1 \\ &\geq \frac{-v_p((y)_\infty) + 1}{p} - \frac{pv_p((x)_\infty)}{p} - 1 \\ &\geq -v_p((y)_\infty) - v_p((x)_\infty), \end{aligned}$$

where we have used that  $i \geq 1$ . A similar calculation shows that  $\sigma_i(W) \subseteq W$  for any  $i$ . □

**Lemma 3.12.** *Let  $T$  be the maximum order of any pole of  $y$  or zero of  $x$ . Then*

$$\sigma_0^\ell(y \, dx) \in \Omega(\sqrt{(y)_\infty} - (x)_0 + \sqrt{(x)_0} + (x)_\infty + \sqrt{(x)_\infty})$$

for  $\ell \geq \lceil \log_p(T) \rceil$ .

*Proof.* As in the proof of [Proposition 3.8](#), any  $\omega \in S_p(y \, dx)$  can have poles only at the poles of  $y \, dx$  or of  $x$ . Writing locally in Laurent series expansions shows that the poles of  $y \, dx$  are all either poles of  $y$  or poles of  $x$ , and in fact  $y \, dx \in \Omega((y)_\infty + (x)_\infty + \sqrt{(x)_\infty})$ . For any  $\omega \in \Omega$ , we compute

$$\sigma_0(\omega) = \mathcal{C}\left(\frac{x^p \omega}{x}\right) = x \mathcal{C}\left(\frac{\omega}{x}\right)$$

and therefore

$$\sigma_0^n(\omega) = x \mathcal{C}^n\left(\frac{\omega}{x}\right)$$

for every  $n \geq 1$ .

Let  $\alpha = (y \, dx)/x$ . We have  $\alpha \in \Omega((y)_\infty + (x)_0 + \sqrt{(x)_\infty})$ . As  $y$  is a power series in  $x$ , it must be the case that  $y$  is a regular function at every zero of  $x$ , so no point can be both a pole of  $y$  and a zero of  $x$ . Let  $P$  be a point that is either a pole of  $y$  or a zero of  $x$ . Thus  $v_P(\alpha) \geq -T$ . Repeatedly applying [Proposition 3.7](#), we see that  $v_p(\mathcal{C}^\ell(\alpha)) \geq -1$  for  $\ell \geq \log_p(T)$ . Therefore  $\mathcal{C}^\ell(\alpha) \in \Omega(\sqrt{(y)_\infty} + \sqrt{(x)_0} + \sqrt{(x)_\infty})$ . As  $\sigma_0^\ell(y \, dx) = x \mathcal{C}^\ell(\alpha)$ , we conclude

$$\sigma_0^\ell(y \, dx) \in \Omega(\sqrt{(y)_\infty} + \sqrt{(x)_0} + \sqrt{(x)_\infty} - (x)_0 + (x)_\infty)$$

as claimed. □

The next lemma handles the repeated action of  $\mathcal{C}$  on differentials with simple poles.

**Lemma 3.13.** *Suppose  $\omega \in K$  has simple poles at points of degrees  $e_1, e_2, \dots, e_n$ . Let  $m$  be the LCM of  $e_1, \dots, e_n$ . Then  $C^{rm}(\omega) - \omega$  is holomorphic (recall  $q = p^r$ ).*

*Proof.* Let  $X'$  be the base change  $X' = X \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$  with base change morphism  $\phi : X' \rightarrow X$ . Let  $K' = \phi^*K$ , which is the constant field extension  $\mathbb{F}_{q^m}K$ . Each place  $P$  of  $K$  which is a pole of  $\omega$  splits completely in the extension to  $K'$  (for example, by [Stichtenoth 2009, Theorem 3.6.3 g] each place  $P'$  lying over  $P$  has residue field equal to  $\mathbb{F}_{q^m}$ ). Therefore the pullback  $\phi^*\omega$  has simple poles at places of degree 1. So  $\mathcal{C}(\phi^*\omega)$  has simple poles at the same places as  $\phi^*\omega$ . At each of these places  $P'$ , we compute

$$\text{res}_{P'}(C^{rm}(\phi^*\omega)) = \text{res}_{P'}(\phi^*\omega)^{(1/p)^{rm}} = \text{res}_{P'}(\phi^*\omega)^{q^{-m}} = \text{res}_{P'}(\phi^*\omega),$$

because the residue lies in  $\mathbb{F}_{q^m}$ , which is fixed under the  $q^m$ -th power map. So  $C^{rm}(\phi^*\omega)$  has simple poles at the same places as  $\phi^*\omega$  with the same residues, and therefore  $C^{rm}(\phi^*\omega) - \phi^*\omega$  is holomorphic. The Cartier operator commutes with pullback, so

$$C^{rm}(\phi^*\omega) - \phi^*\omega = \phi^*(C^{rm}(\omega) - \omega)$$

and we conclude that  $C^{rm}(\omega) - \omega$  is also holomorphic.  $\square$

Using the preceding lemmas, we now prove [Theorem 1.2](#).

*Proof of Theorem 1.2.* Let  $V = \Omega((y)_\infty + (x)_\infty + \sqrt{(x)_\infty})$  and  $W = \Omega((y)_\infty) + (x)_\infty$ . By [Lemma 3.11](#),  $\sigma_i(y dx) \in W$  for every  $i > 0$ , and  $W$  is  $\sigma_i$ -invariant for every  $i$ . So we have

$$|N_q(\mathbf{a})| = |S_q(y dx)| \leq |S_p(y dx)| \leq 1 + |\{\sigma_0^n(y dx) : n \geq 1\}| + |W|.$$

By Riemann–Roch,  $\dim_{\mathbb{F}_q} W = \deg((y)_\infty + (x)_\infty) + g - 1 \leq h + d + g - 1$ . The remainder of the proof will handle the orbit of  $y dx$  under  $\sigma_0$ .

Let  $T$  be the maximum order of any pole of  $y$  or zero of  $x$ . Let

$$D = \sqrt{(y)_\infty} + \sqrt{(x)_0} + \sqrt{(x)_\infty}.$$

By [Lemma 3.12](#), for  $n \geq \lceil \log_p(T) \rceil$ , we have that  $\sigma_0^n(y dx) \in \Omega(D - (x))$ . Let  $\alpha = x^{-1}\sigma_0^{\lceil \log_p(T) \rceil}(y dx)$ . So  $\alpha \in \Omega(D)$ , that is,  $\alpha$  has simple poles at points that are either poles of  $y$ , poles of  $x$ , or zeroes of  $x$ . We have seen that  $x\mathcal{C}^n(\alpha) = \sigma_0^n(x\alpha)$ . It follows that

$$|\{\mathcal{C}^n(\alpha) : n \geq 0\}| = |\{\sigma_0^n(y dx) : n \geq \log_p(T)\}|.$$

Let  $m$  be the LCM of the degrees of the points at which  $\alpha$  has a pole. By [Lemma 3.13](#),  $C^{rm}(\alpha) - \alpha$  is holomorphic. The space of holomorphic differentials is invariant under  $\mathcal{C}$ , so the orbit of  $\alpha$  under  $\mathcal{C}$  is contained in the set

$$\{\mathcal{C}^k(\alpha) + \eta : 0 \leq k < rm \text{ and } \eta \in \Omega(0)\}.$$

This set has size at most  $rm|\Omega(0)| = rmq^g$ . Thus

$$|\{\sigma_0^n(\omega) : n \geq 1\}| \leq \lceil \log_p(T) \rceil + rmq^g.$$

We now need to estimate  $m$ .

Let  $L(n)$  be Landau’s function, that is, the largest LCM of all partitions of  $n$ , or equivalently the maximum order of an element in the symmetric group of order  $n$ . Recall from the proof of [Corollary 3.10](#) that  $\deg(y)_\infty = h$  and  $\deg(x)_\infty = d$ . We have

$$\sum_{v_p(y) < 0} \deg P \leq \sum_{v_p(y) < 0} -v_p(y) \deg P = \deg(y_\infty) = h,$$

and it follows in the same way that  $\sum_{v_p(x) < 0} \deg P \leq d$  and  $\sum_{v_p(x) > 0} \deg P \leq d$ . Therefore  $m \leq L(h)L(d)^2$ . It is clear that  $L(a)L(b) \leq L(a + b)$  for all  $a$  and  $b$ , so  $m \leq L(h + 2d)$ . So

$$|\{\sigma_0^n(y \, dx) : n \geq 1\}| \leq \lceil \log_p(T) \rceil + rL(h + 2d)q^g.$$

Therefore  $|\mathcal{S}_p(y \, dx)| \leq 1 + \lceil \log_p(T) \rceil + rL(h + 2d)q^g + q^{h+d+g-1}$ .

It remains to show that the quantity

$$\frac{1 + \lceil \log_p(T) \rceil + rL(h + 2d)q^g}{q^{h+d+g-1}}$$

decays to zero as any of  $q$ ,  $h$ ,  $d$ , or  $g$  grow to  $\infty$ . This follows easily from the fact that  $g \geq 0$  and  $h + d \geq 2$  for any algebraic curve, the simple bound on Landau’s function

$$L(n) \leq \exp((1 + o(1))\sqrt{n \log n})$$

from [\[Massias et al. 1989\]](#), and the fact that  $T \leq \max(h, d)$ . □

The forward-reading complexity bound of [Theorem 1.5](#) follows as an easy corollary.

*Proof of [Theorem 1.5](#).* Let  $V = \Omega((y)_\infty + (x)_\infty + \sqrt{(x)_\infty})$  and let  $\lambda \in V^*$  be the linear functional that maps  $\omega$  to the constant term of the power series  $\frac{\omega}{dx}$ . We have  $\dim_{\mathbb{F}_q} V \leq h + 2d + g - 1$ , so

$$|N_q^f(\mathbf{a})| = |\mathcal{S}_q^T(\lambda)| \leq |V^*| \leq q^{h+2d+g-1}$$

by [Proposition 2.4](#). □

We now show that [Theorem 1.2](#) is qualitatively sharp for the power series expansions of rational functions, that is, it is sharp if we replace the “error term”  $o(1)$  by zero.

**Proposition 3.14.** *For every prime power  $q$  and every positive integer  $h \geq 1$ , there exists  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_q[[x]]$  with  $\deg y = 1$  and  $h(y) = h$  (and therefore  $g = 0$ ) such that  $N_q(\mathbf{a}) \geq q^h$ .*

*Proof.* Let  $f = x^h + c_{h-1}x^{h-1} + \cdots + c_1x + c_0 \in \mathbb{F}_q[x]$  be any primitive polynomial, that is, such that a root of  $f$  generates  $\mathbb{F}_{q^h}^\times$ . Let  $y = f^{-1} - 1 \in \mathbb{F}_q[[x]]$ . The coefficient sequence  $\mathbf{a}$  of  $y$  satisfies the linear recurrence relation

$$c_0\mathbf{a}(n) + c_1\mathbf{a}(n-1) + \cdots + c_{h-1}\mathbf{a}(n-h+1) + \mathbf{a}(n-h) = 0$$

and  $\mathbf{a}$  is eventually periodic with minimal period  $q^h - 1$  [Lidl and Niederreiter 1994, Theorem 6.28]. We have  $\deg y = 1$  and  $h(y) = h$ , so the curve  $X$  is  $\mathbb{P}^1$ , with  $K = \mathbb{F}_q(x)$  and  $g = 0$ .

Note that  $(y)_\infty = (f)_0$  is a single point of degree  $h$ . Let  $P_\infty$  be the pole of  $x$ , which is distinct from  $(f)_0$ . We compute

$$(f^{-1} dx) = hP_\infty - (f)_0 - 2P_\infty = (h-2)P_\infty - (f)_0,$$

so  $f^{-1} dx$  has at most two poles: a simple pole at  $(f)_0$  of degree  $h$ , and if  $h = 1$ , a simple pole at  $P_\infty$  of degree 1. By Lemma 3.13,  $\mathcal{C}^{rh}(y dx) - f^{-1} dx = \mathcal{C}^{rh}(f^{-1} dx) - f^{-1} dx$  is holomorphic (note  $\mathcal{C}(dx) = 0$  by Proposition 3.7). As  $X$  has genus 0, it carries no nonzero holomorphic differentials, so  $\mathcal{C}^{rh}(y dx) = f^{-1} dx$ .

Let  $\mathbf{b}$  be the coefficient sequence of  $f^{-1}$ . The sequence  $\mathbf{b}$  satisfies a linear recurrence relation of degree  $h$  and has period  $q^h - 1$ , so it must be the case that all possible strings of  $h$  elements in  $\mathbb{F}_q$  except for the string  $(0, \dots, 0)$  occur in  $\mathbf{b}$  within the first  $q^h - 1$  terms. For each  $0 \leq c \leq q - 1$ , a certain  $r$ -fold composition of  $\Lambda_i$  operators  $s \in S_q$  gives  $s(f^{-1}) = \sum_{n=0}^{\infty} \mathbf{b}(qn + c)x^n$ , so

$$\Lambda_0^{rh} s(f^{-1}) = \sum_{n=0}^{\infty} \mathbf{b}(q^h n + c)x^n = \sum_{n=c}^{\infty} \mathbf{b}(n)x^n,$$

by the periodicity of  $\mathbf{b}$ . So there are at least  $q^h - 1$  distinct power series in  $S_q(f^{-1})$ .

Let  $V = \Omega((f)_0 + P_\infty)$ . We have  $(f^{-1} dx) \in V$ , and  $\dim_{\mathbb{F}_q} V = h$  by Riemann–Roch. A calculation with properties of  $\mathcal{C}$  and orders of poles shows that  $V$  is  $\sigma_i$ -invariant for any  $i \in \{0, \dots, p-1\}$ , so  $S_q(f^{-1} dx) \subseteq V$ . The counting argument from the previous paragraph shows that the orbit  $S_q(f^{-1} dx)$  comprises all nonzero elements of  $V$ . (In fact, it is not hard to show that  $\sigma_i|_V$  is invertible for each  $i$ , so the action of  $S_p$  on  $V$  is a group action with precisely two orbits:  $\{0\}$  and  $V \setminus \{0\}$ .) Note that  $y dx \notin V$ , for if  $y dx$  were in  $V$ , then  $dx$  would be also, but  $(dx) = -2P_\infty$ . So  $y \notin S_q(f^{-1})$ , which establishes the lower bound  $|S_q(y)| = N_q(\mathbf{a}) \geq q^h - 1 + 1 = q^h$ .  $\square$

**3C. Variation mod primes.** Let  $K$  be a number field and  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in K[[x]]$ . If the prime  $\mathfrak{p}$  of  $K$  is such that  $v_{\mathfrak{p}}(\mathbf{a}(n)) \geq 0$  for all  $n$ , let  $\mathbf{a}_{\mathfrak{p}}$  denote the reduction of  $\mathbf{a} \bmod \mathfrak{p}$ , and let  $y_{\mathfrak{p}} = \sum_{n=0}^{\infty} \mathbf{a}_{\mathfrak{p}}(n)x^n$  be the reduced power series with coefficients in the residue field  $k(\mathfrak{p})$ .

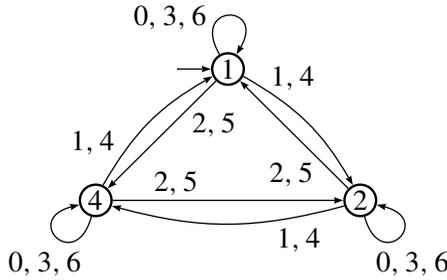
Suppose  $y$  is algebraic over  $K(x)$ . By a theorem of Eisenstein [1852], there are only finitely many primes  $\mathfrak{p}$  such that  $v_{\mathfrak{p}}(\mathbf{a}(n)) < 0$  for some  $n$  (see [Schmidt 1990] for exposition). So the sequence  $\mathbf{a}_{\mathfrak{p}}$  is defined for all but finitely many  $\mathfrak{p}$ , and by Christol's theorem it is  $|k(\mathfrak{p})|$ -automatic (it is an easy observation that the reduction mod  $\mathfrak{p}$  of an algebraic function is algebraic). An extension of our main question is how the algebraic nature of  $y$  affects the complexity  $N_{|k(\mathfrak{p})|}(\mathbf{a}_{\mathfrak{p}})$  as the prime  $\mathfrak{p}$  varies. Theorem 3.15 answers this question in the case that the complexities are bounded at all primes; in this case  $y$  must have a very special form. Note that we do not need to assume that  $y$  is algebraic in the statement of the theorem. To simplify notation, we will write  $N_{\mathfrak{p}}(\mathbf{a}_{\mathfrak{p}})$  in place of  $N_{|k(\mathfrak{p})|}(\mathbf{a}_{\mathfrak{p}})$ .

**Theorem 3.15.** *Let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in K[[x]]$ . Then  $N_{\mathfrak{p}}(\mathbf{a}_{\mathfrak{p}})$  and  $N_{\mathfrak{p}}^f(\mathbf{a}_{\mathfrak{p}})$  are bounded independently of  $\mathfrak{p}$  if and only if  $y$  is a rational function with at worst simple poles that occur at roots of unity (except possibly for a pole at  $\infty$ , which may be of any order).*

*Proof.* It suffices to prove the theorem for reverse-reading complexity, as  $N_{\mathfrak{p}}^f(\mathbf{a}) \leq p^{N_{\mathfrak{p}}(\mathbf{a})}$  for any sequence  $\mathbf{a}$  by Proposition 2.4. Assume that  $N_{\mathfrak{p}}(\mathbf{a})$  is uniformly bounded for all  $\mathfrak{p}$  (such that it is defined). Then the coefficient sequence  $\mathbf{a}$  assumes a bounded number of values under reduction mod  $\mathfrak{p}$  regardless of  $\mathfrak{p}$ , and so  $\mathbf{a}$  assumes finitely many values in  $K$ . Let  $A$  be this finite subset of  $K$ .

Choose two primes  $\mathfrak{p}$  and  $\mathfrak{q}$  such that  $|k(\mathfrak{p})|$  and  $|k(\mathfrak{q})|$  are multiplicatively independent integers (i.e.,  $\text{char } k(\mathfrak{p}) \neq \text{char } k(\mathfrak{q})$ ) and all elements of  $A$  are distinct both mod  $\mathfrak{p}$  and mod  $\mathfrak{q}$  (this is possible because only finitely many primes divide distances between distinct elements of  $A$ ). The reduced power series  $y_{\mathfrak{p}} \in k(\mathfrak{p})[[x]]$  and  $y_{\mathfrak{q}} \in k(\mathfrak{q})[[x]]$  are both algebraic by Christol's theorem. So there exist injections  $i_{\mathfrak{p}} : A \hookrightarrow k(\mathfrak{p})$  and  $i_{\mathfrak{q}} : A \hookrightarrow k(\mathfrak{q})$  such that the sequence  $\mathbf{b}(n) = i_{\mathfrak{p}}(\mathbf{a}(n))$  is  $|k(\mathfrak{p})|$ -automatic and the sequence  $\mathbf{c}(n) = i_{\mathfrak{q}}(\mathbf{a}(n))$  is  $|k(\mathfrak{q})|$ -automatic. Therefore  $\mathbf{a}$  is both  $|k(\mathfrak{p})|$ -automatic and  $|k(\mathfrak{q})|$ -automatic. By Cobham's theorem [Allouche and Shallit 2003, Theorem 11.2.2],  $\mathbf{a}$  is an eventually periodic sequence of some period  $m$ , so  $y$  is a rational function of the form  $y = f/(1 - x^m)$  for some polynomial  $f$ . So the (finite) poles of  $y$  are simple and occur at roots of unity.

Conversely, assume that the (finite) poles of  $y$  are simple and occur at roots of unity. Therefore  $y = f/(1 - x^m)$  for some  $m$  and  $f \in K[x]$ , and the coefficient sequence  $\mathbf{a}$  is eventually periodic of (possibly nonminimal) period  $m$ , that is, there is some  $c$  such that  $\mathbf{a}(n + m) = \mathbf{a}(n)$  for all  $n > c$ . In particular,  $\mathbf{a}$  assumes finitely many values. An easy decimation argument now shows that  $N_{\mathfrak{p}}(\mathbf{a})$  is uniformly



**Figure 4.** 7-DFAO generating powers of 2 mod 7.

bounded for all primes. Suppose  $|k(\mathfrak{p})| = p^r$  and assume that  $p^r > c$  (which excludes only finitely many  $\mathfrak{p}$ ). For any  $i \geq 1$  and  $j \in \{0, \dots, p^{ri} - 1\}$ , the subsequences  $\mathbf{a}(p^{ri}n + j)$  are periodic of period  $m$  beginning with the second term, and they assume the same finite set of values as  $\mathbf{a}$ . There are clearly only finitely many sequences that fit this description. So the size of the  $p^r$ -kernel of  $\mathbf{a}$ , and therefore  $N_{\mathfrak{p}}(\mathbf{a})$ , is bounded independently of  $p$ .  $\square$

### 4. Examples

We give three detailed examples of computing the state complexity of an automatic sequence. Examples 4.2 and 4.3 in particular show the usefulness of the algebro-geometric approach.

**Example 4.1.** 
$$y = \frac{1}{1-2x}.$$

Let  $p$  be odd. Let  $\mathbf{a}(n) = 2^n \bmod p$  and  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_p[[x]]$ . We have  $y(1 - 2x) = 1$ , so  $y$  has degree 1, height 1, and genus 0. By Theorem 1.2,  $N_p(\mathbf{a}) \leq (1 + o_p(1))p$ . We compute  $\Lambda_i(y) = 2^i y$ , so  $S_p(y) = \{2^i y : i \geq 0\}$ , and  $N_p(\mathbf{a}) = \text{ord}_p(2)$ . So in fact

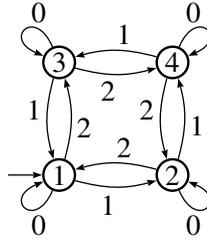
$$\lceil \log_2(p) \rceil \leq N_p(\mathbf{a}) \leq p - 1.$$

If there are infinitely many Mersenne primes, the lower bound is sharp infinitely often, and if Artin’s conjecture is true, the upper bound is sharp infinitely often.

The sequence  $\mathbf{a}$  has a one-dimensional  $p$ -representation where  $\phi(i) : v \mapsto 2^i v$ . Each  $\phi(i)$  can be written as a (symmetric)  $1 \times 1$  matrix, so the  $p$ -antirepresentation on  $V^*$  is the same as the original representation, and  $N_p^f(\mathbf{a}) = N_p(\mathbf{a})$ . From the automata point of view, this is the obvious fact that the same DFAO outputs  $\mathbf{a}$  in both the forward-reading and reverse-reading conventions. The transition diagram of the DFAO for  $p = 7$  is given in Figure 4.

**Example 4.2.** 
$$y = \frac{1}{\sqrt{1-4x}}.$$

Let  $p$  be an odd prime. Let  $\mathbf{a}(n)$  be the central binomial coefficient  $\binom{2n}{n}$  reduced mod  $p$  and let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n \in \mathbb{F}_p[[x]]$ . From Newton’s formula for the binomial



**Figure 5.** 5-DFAO generating the central binomial coefficients mod 5.

series, we have  $y^2(1 - 4x) = 1$ . So  $y$  has degree 2, height 1, and genus 0, and  $N_p(\mathbf{a}) \leq (1 + o_p(1))p^2$ . We show that  $N_p(\mathbf{a}) = N_p^f(\mathbf{a}) = p$ . (A calculation verifies that  $N_2^f(\mathbf{a}) = N_2(\mathbf{a}) = 2$  as well.)

Let  $X$  be the curve defined by  $y^2(1 - 4x) = 1$ . We have  $x = \frac{1}{4} - y^{-2}$ , so  $X = \mathbb{P}^1(\mathbb{F}_p)$ , parametrized by  $y$ . Let  $P_0$  and  $P_\infty$  be the zero and pole of  $y$ , and let  $\omega = y dx$ . A computation gives  $dx = -2y^{-3} dy$ , so

$$(\omega) = -2(P_0) \quad \text{and} \quad (x) = (P_2) + (P_{-2}) - 2(P_0).$$

For any  $i \in \{0, \dots, p - 1\}$ ,

$$v_{P_0}(x^{p-1-i}\omega) = (p - 1 - i)v_{P_0}(x) + v_{P_0}(\omega) > (p - 1)(-2) - 2 = -2p.$$

So  $v_{P_0}(\sigma_i(\omega)) = v_{P_0}(C(x^{p-1-i}\omega))$  is either 0,  $-1$ , or  $-2$ , and  $P_0$  is the only point at which  $\sigma_i(\omega)$  can have a pole. A canonical divisor of  $X$  has degree  $-2$ , so by Riemann–Roch,  $\Omega(2P_0)$  is one-dimensional,  $S_p(\omega) \subseteq \mathbb{F}_p\omega$ , and  $N_p(\mathbf{a}) \leq p$ .

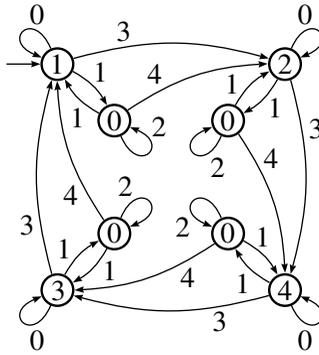
More explicitly, as  $S_p(\omega)$  sits in a one-dimensional vector space we have  $\sigma_i(\omega) = c_i\omega$  for some  $c_i \in \mathbb{F}_p$ . As  $\sigma_i(\omega) = \Lambda_i(y) dx$  and the constant term of  $y$  is 1,  $c_i$  is equal to the constant term of  $\Lambda_i(y)$ , which is  $\binom{2i}{i}$ . So  $\sigma_i(\omega) = \binom{2i}{i}\omega$ . Equating coefficients gives

$$\binom{2(pn+i)}{pn+i} \equiv \binom{2i}{i} \binom{2n}{n} \pmod{p}.$$

(Amusingly, this gives a roundabout argument that recovers a special case of the classical theorem of Lucas on binomial coefficients mod  $p$ .)

To see that  $N_p(\mathbf{a})$  is exactly  $p$ , note that  $\mathbf{a}(1) = 2$ , and that for any odd prime  $q$ ,  $\mathbf{a}((q + 1)/2)$  is the first central binomial coefficient divisible by  $q$ . This shows that the subgroup of  $\mathbb{F}_p^\times$  generated by all nonzero central binomial coefficients mod  $p$  contains all primes less than  $p$  and therefore is all of  $\mathbb{F}_p^\times$ , and furthermore  $\mathbf{a}((p + 1)/2) = 0$ .

As in the previous example, the fact that  $S_p(\omega)$  lies in a one-dimensional vector space verifies that  $N_p^f(\mathbf{a}) = N_p(\mathbf{a})$  for all  $p$ . The transition diagrams for the automata that output  $\mathbf{a}$  have nicely symmetric structures. Figure 5 displays the DFAO for  $p = 5$ —all undrawn transitions, which are on the inputs 3, 4, and 5, go to an undrawn trap state, which outputs zero.



**Figure 6.** Reverse-reading 5-DFAO generating the coefficients of  $(1 - 4x^3)^{-1/2} \pmod 5$ .

**Example 4.3.**

$$y = \frac{1}{\sqrt{1-4x^3}}.$$

Let  $p \notin \{2, 3\}$ . Let  $\mathbf{a}$  be the coefficient sequence of the series  $1/\sqrt{1-4x^3} \in \mathbb{Q}[[x]]$  reduced mod  $p$ , so that  $\mathbf{a}(3n) = \binom{2n}{n} \pmod p$  and  $\mathbf{a}(n) = 0$  if  $n$  is not a multiple of 3. Let  $y = \sum_{n=0}^{\infty} \mathbf{a}(n)x^n$ . We have  $y^2(1-4x^3) = 1$ , so  $y$  is of degree 2, height 3, and genus 1, and  $N_p(\mathbf{a}) \leq (1 + o_p(1))p^5$ . We show that  $N_p(\mathbf{a}) = 2p - 1$ .

Let  $C$  be the curve defined by  $Y^2(Z^3 - 4W^3) = Z^5$  in  $\mathbb{P}^2$ . This curve is singular, so define the smooth (elliptic) curve  $X$  by  $Y^2Z = Z^3 - 4W^3$ . The morphism  $\phi : X \rightarrow C$ , defined in homogeneous coordinates by

$$\phi : [W : Y : Z] \mapsto [WY : Z^2 : YZ],$$

gives the normalization of  $C$ . The forms  $[Y : Z]$  and  $[W : Z]$  are maps from  $C$  to  $\mathbb{P}^1$ , so we can consider them as elements of  $\mathbb{F}_p(C)$ . Let  $y = \phi^*[Y : Z]$  and  $x = \phi^*[W : Z]$ . So we have  $y^2(1-4x^3) = 1$ . Let  $\omega = y dx$  and let  $P_\infty$  be the point on  $X$  written as  $[0 : 1 : 0]$  in homogeneous coordinates. The following are easy computations, where  $P, Q,$  and  $R$  are some points of  $X$  that we do not need to compute explicitly:

$$\begin{aligned} (y) &= 3P_\infty - P - Q - R, \\ (x) &= [0 : 1 : 1] + [0 : -1 : 1] - 2P_\infty, \\ (dx) &= -(y). \end{aligned}$$

In particular,  $(\omega) = 0$ . Our usual computation for the possible orders of poles of  $\sigma_i(\omega)$  shows that  $\mathcal{S}_p(\omega) \subseteq \Omega(2P_\infty)$ , which has dimension 2 with  $\{\omega, x\omega\}$  as a basis. We use properties of  $C$  to compute the action of  $\mathcal{S}_p$  on the basis.

As  $y^2 = 1/(1 - 4x^3)$ , we have

$$\begin{aligned}\sigma_i(\omega) &= \mathcal{C}(x^{p-i-1} y dx) \\ &= \mathcal{C}\left(x^{p-i-1} \frac{y^p}{y^{p-1}} dx\right) \\ &= y\mathcal{C}(x^{p-i-1} (1 - 4x^3)^{(p-1)/2} dx) \\ &= y\mathcal{C}\left(\sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{k} (-4)^k x^{3k+p-i-1} dx\right).\end{aligned}$$

So  $\sigma_i(\omega)$  is nonzero precisely when there is some  $0 \leq k \leq (p-1)/2$  with

$$3k + p - i - 1 \equiv p - 1 \pmod{p},$$

that is, when  $3k \equiv i \pmod{p}$  has a solution  $k$  with  $0 \leq k \leq (p-1)/2$ . If there is such a  $k$ , then it is unique, and  $3k - i \leq 3(p-1)/2 < 2p$ , so either  $3k = i$ , in which case

$$\sigma_i(\omega) = \binom{(p-1)/2}{i/3} (-4)^{i/3} \omega,$$

or  $3k = i + p$ , in which case

$$\sigma_i(\omega) = \binom{(p-1)/2}{(i+p)/3} (-4)^{(i+p)/3} x\omega.$$

This shows that  $\mathcal{S}_p(\omega) \subseteq \mathbb{F}_p\omega \cup \mathbb{F}_p x\omega$ . Also, the fact that  $\sigma_i(\omega) = \Lambda_i(y) dx$  proves the identity

$$\binom{(p-1)/2}{k} (-4)^k \equiv \binom{2k}{k} \pmod{p}$$

for all  $k$ .

With this calculation we can explicitly write the restriction of  $\sigma_i$  to  $\Omega(2P_\infty)$  by computing its action on the basis  $\{\omega, x\omega\}$ . So far we have only computed the action of  $\sigma_i$  on  $\omega$ , but for  $i \geq 1$  we have  $\sigma_i(x\omega) = \sigma_{i-1}(\omega)$ , and  $\sigma_0(x\omega) = \mathcal{C}(x^p\omega) = x\mathcal{C}(\omega) = x\sigma_{p-1}(\omega)$ . We have

$$\sigma_i(\omega) = \begin{cases} \binom{2i/3}{i/3} \omega & i \equiv 0 \pmod{3}, \\ \binom{2(i+p)/3}{(i+p)/3} x\omega & i \equiv -p \pmod{3}, \\ 0 & i \equiv p \pmod{3}, \end{cases}$$

and

$$\sigma_i(x\omega) = \begin{cases} \binom{2(i-1)/3}{(i-1)/3} \omega & i \equiv 1 \pmod{3}, \\ \binom{2(i-1+p)/3}{(i-1+p)/3} x\omega & i \equiv 1 - p \pmod{3}, \\ 0 & i \equiv 1 + p \pmod{3}, \end{cases}$$

where  $0, p, -p$  are distinct mod  $p$  because  $p > 3$ .

Incidentally, it follows from our computation that  $\mathcal{C}(\omega) = 0$  if and only if  $p \equiv 2 \pmod{3}$ , which shows that these are precisely the primes for which the elliptic curve  $X$  is supersingular, as the classical Hasse invariant is the rank of the restriction of the Cartier operator to the space of holomorphic differentials. See [Silverman 2009, Section 5.4].

Examining the binomial coefficients that appear in the formula for  $\sigma_i(\omega)$  shows that  $\binom{2k}{k}$  appears as a coefficient on  $\omega$  for  $0 \leq k \leq \lfloor p/3 \rfloor$ , and as a coefficient on  $x\omega$  for  $\lfloor p/3 \rfloor + 1 \leq k \leq (2p-1)/3$ . As in Example 4.2, the values of  $\binom{2k}{k} \pmod{p}$  for  $0 \leq k \leq (p-1)/2$  generate the multiplicative group of  $\mathbb{F}_p^\times$ , and we have  $\sigma_1(x\omega) = \omega$ . This is already enough to show that  $\mathcal{S}_p(\omega) = \mathbb{F}_p\omega \cup \mathbb{F}_p x\omega$ , so  $N_p(\mathbf{a}) = 2p - 1$ .

For  $p = 5$ , the reverse-reading 5-DFAO that outputs  $\mathbf{a}$  is pictured in Figure 6. As usual, any undrawn transitions lead to a trap state that outputs 0.

**Acknowledgements.** The author would like to thank David Speyer for first exploring this striking link between automata and geometry and for allowing an exposition of his work in [Speyer 2010]. The author also thanks Eric Bach and Jeffrey Shallit for many helpful conversations related to the topics in the paper, and the referee for a careful reading of the paper and helpful comments. Diagrams of automata were produced using the VauCanSon-G Latex package of Sylvain Lombardy and Jacques Sakarovitch.

## References

- [Adamczewski and Bell 2012] B. Adamczewski and J. P. Bell, “On vanishing coefficients of algebraic power series over fields of positive characteristic”, *Invent. Math.* **187**:2 (2012), 343–393. [MR](#) [Zbl](#)
- [Adamczewski and Bell 2013] B. Adamczewski and J. P. Bell, “Diagonalization and rationalization of algebraic Laurent series”, *Ann. Sci. Éc. Norm. Supér.* (4) **46**:6 (2013), 963–1004. [MR](#) [Zbl](#)
- [Allouche and Shallit 2003] J.-P. Allouche and J. Shallit, *Automatic sequences*, Cambridge University Press, 2003. [MR](#) [Zbl](#)
- [Berstel and Reutenauer 1988] J. Berstel and C. Reutenauer, *Rational series and their languages*, EATCS Monographs on Theoretical Computer Science **12**, Springer, 1988. [MR](#) [Zbl](#)
- [Brzozowski 1963] J. A. Brzozowski, “Canonical regular expressions and minimal state graphs for definite events”, pp. 529–561 in *Proc. Sympos. Math. Theory of Automata* (New York, 1962), Polytechnic Press, Brooklyn, NY, 1963. [MR](#) [Zbl](#)
- [Cartier 1957] P. Cartier, “Une nouvelle opération sur les formes différentielles”, *C. R. Acad. Sci. Paris* **244** (1957), 426–428. [MR](#) [Zbl](#)
- [Christol 1979] G. Christol, “Ensembles presque périodiques  $k$ -reconnaissables”, *Theoret. Comput. Sci.* **9**:1 (1979), 141–145. [MR](#) [Zbl](#)
- [Christol et al. 1980] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, “Suites algébriques, automates et substitutions”, *Bull. Soc. Math. France* **108**:4 (1980), 401–419. [MR](#) [Zbl](#)
- [Derksen 2007] H. Derksen, “A Skolem–Mahler–Lech theorem in positive characteristic and finite automata”, *Invent. Math.* **168**:1 (2007), 175–224. [MR](#) [Zbl](#)
- [Eilenberg 1974] S. Eilenberg, *Automata, languages, and machines*, vol. A, Pure and Applied Mathematics **58**, Academic Press, New York, 1974. [MR](#) [Zbl](#)

- [Eisenstein 1852] G. Eisenstein, “Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen”, *Preuss. Akad. d. Wissensch. Berlin* (1852), 441–443. reprinted as pp. 765–767 in his *Mathematische Werke*, vol. II, Chelsea, New York, 1975. [MR](#) [Zbl](#)
- [Fresnel et al. 2000] J. Fresnel, M. Koskas, and B. de Mathan, “Automata and transcendence in positive characteristic”, *J. Number Theory* **80**:1 (2000), 1–24. [MR](#) [Zbl](#)
- [Harase 1988] T. Harase, “Algebraic elements in formal power series rings”, *Israel J. Math.* **63**:3 (1988), 281–288. [MR](#) [Zbl](#)
- [Harase 1989] T. Harase, “Algebraic elements in formal power series rings, II”, *Israel J. Math.* **67**:1 (1989), 62–66. [MR](#) [Zbl](#)
- [Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, 1977. [MR](#) [Zbl](#)
- [Lidl and Niederreiter 1994] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, 1st ed., Cambridge University Press, 1994. [MR](#) [Zbl](#)
- [Massias et al. 1989] J.-P. Massias, J.-L. Nicolas, and G. Robin, “Effective bounds for the maximal order of an element in the symmetric group”, *Math. Comp.* **53**:188 (1989), 665–678. [MR](#) [Zbl](#)
- [Salomaa and Soittola 1978] A. Salomaa and M. Soittola, *Automata-theoretic aspects of formal power series*, Springer, 1978. [MR](#) [Zbl](#)
- [Schmidt 1990] W. M. Schmidt, “Eisenstein’s theorem on power series expansions of algebraic functions”, *Acta Arith.* **56**:2 (1990), 161–179. [MR](#) [Zbl](#)
- [Serre 1958] J.-P. Serre, “Sur la topologie des variétés algébriques en caractéristique  $p$ ”, pp. 24–53 in *Symposium internacional de topología algebraica* (Mexico City, 1956), Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958. [MR](#) [Zbl](#)
- [Shallit 2009] J. Shallit, *A second course in formal languages and automata theory*, Cambridge University Press, 2009. [Zbl](#)
- [Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. [MR](#) [Zbl](#)
- [Speyer 2010] D. Speyer, “Christol’s theorem and the Cartier operator”, 2010, available at <https://sbseminar.wordpress.com/2010/02/11/christols-theorem-and-the-cartier-operator/>.
- [Stichtenoth 2009] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics **254**, Springer, 2009. [MR](#) [Zbl](#)

Communicated by Kiran S. Kedlaya

Received 2016-06-20

Revised 2016-11-20

Accepted 2016-12-19

[andrewbridy@math.tamu.edu](mailto:andrewbridy@math.tamu.edu)

*Department of Mathematics, Texas A&M University,  
Department of Mathematics, Mailstop 3368,  
College Station, TX 77843, United States*

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Martin Olsson	University of California, Berkeley, USA
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Hélène Esnault	Freie Universität Berlin, Germany	Michael Rapoport	Universität Bonn, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Victor Reiner	University of Minnesota, USA
Hubert Flenner	Ruhr-Universität, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Christopher Skinner	Princeton University, USA
Joseph Gubeladze	San Francisco State University, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Roger Heath-Brown	Oxford University, UK	J. Toby Stafford	University of Michigan, USA
Craig Huneke	University of Virginia, USA	Pham Huu Tiep	University of Arizona, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Ravi Vakil	Stanford University, USA
János Kollár	Princeton University, USA	Michel van den Bergh	Hasselt University, Belgium
Yuri Manin	Northwestern University, USA	Marie-France Vignéras	Université Paris VII, France
Philippe Michel	École Polytechnique Fédérale de Lausanne	Kei-Ichi Watanabe	Nihon University, Japan
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2017 is US \$325/year for the electronic version, and \$520/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFLOW<sup>®</sup> from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2017 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 11    No. 3    2017

---

<a href="#">The umbral moonshine module for the unique unimodular Niemeier root system</a>	505
JOHN F. R. DUNCAN and JEFFREY A. HARVEY	
<a href="#">Geometry on totally separably closed schemes</a>	537
STEFAN SCHRÖER	
<a href="#">The sixth moment of automorphic <math>L</math>-functions</a>	583
VORRAPAN CHANDEE and XIANNAN LI	
<a href="#">A duality in Buchsbaum rings and triangulated manifolds</a>	635
SATOSHI MURAI, ISABELLA NOVIK and KEN-ICHI YOSHIDA	
<a href="#">Analytic functions on tubes of nonarchimedean analytic spaces</a>	657
FLORENT MARTIN	
<a href="#">Automatic sequences and curves over finite fields</a>	685
ANDREW BRIDY	
<a href="#">On an analogue of the Ichino–Ikeda conjecture for Whittaker coefficients on the metaplectic group</a>	713
EREZ LAPID and ZHENGYU MAO	