ALGEBRAIC POWER SERIES AND THEIR AUTOMATIC COMPLEXITY II: MODULO PRIME POWERS

ERIC ROWLAND AND REEM YASSAWI

Abstract. Christol and, independently, Denef and Lipshitz showed that an algebraic sequence of p-adic integers (or integers) is p-automatic when reduced modulo p^α. Previously, the best known bound on the minimal automaton size for such a sequence was doubly exponential in α. We improve this bound to the order of $p^{\alpha^3 hd}$, where h and d are the height and degree of the minimal annihilating polynomial. We achieve this bound by showing that all states in the automaton are naturally represented in a new numeration system. This significantly restricts the set of possible states. Since our approach embeds algebraic sequences as diagonals of rational functions, we also obtain bounds more generally for diagonals of multivariate rational functions.

1. Introduction

Christol's theorem [5, 7] states that a power series $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{F}_q[\![x]\!]$ with coefficients in a finite field is algebraic if and only if its sequence of coefficients $a(n)_{n\geq 0}$ is q-automatic. Given a nonzero polynomial $P \in \mathbb{F}_q[x, y]$ such that $P(x, F) = 0$, the proof of Christol's theorem allows one to compute an automaton that outputs $a(n)$ when fed the standard base-q representation of n. Bridy [4] gave an upper bound on the size of this automaton in terms of the size of P. Namely, define the *height* $h := \deg_x P$ and *degree* $d := \deg_y P$. Then the number of states is in $(1 + o(1))q^{hd}$ as q, h, or d gets large. In a previous article, Stipulanti and the authors [16] gave a new proof of Bridy's bound.

Christol [6] and, using a different approach, Denef and Lipshitz [8] proved a generalization of Christol's theorem for power series with coefficients in $\mathbb{Z}$ or, more generally, the set $\mathbb{Z}_p$ of p-adic integers where p is a prime. Namely, if $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!]$ is algebraic, then the sequence $(a(n) \bmod p^\alpha)_{n\geq 0}$ of elements in the ring $\mathcal{R}_{p^\alpha} := \mathbb{Z}/p^\alpha\mathbb{Z}$ is p-automatic for each $\alpha \geq 1$. In this article, we bound the size of the minimal automaton generating this sequence. Here and throughout this article, automata read the least significant digit first. From one of the constructions of Denef and Lipshitz [8, Remark 6.6], one obtains that the number of states is at most $p^{\alpha(p^{\alpha-1}\max(h,d)+1)^2}$ [17, Remark 2.2]. This bound is doubly exponential in α. The techniques from [16] can be generalized to give a bound in this setting, but this bound is also doubly exponential. In this article, we significantly reduce the bound to roughly $p^{\alpha^3 hd}$. This reduction is achieved primarily by identifying new structure in the representations of the states of the automaton. To state the main results, we introduce the following terminology.

Date: August 1, 2024.

2020 *Mathematics Subject Classification.* 11B85, 13F25.

The second author was supported by the EPSRC, grant number EP/V007459/2.

Definition. Let $P \in \mathbb{Z}_p[x,y]$ such that $P(0,0) = 0$ and $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$. The *Furstenberg series* associated with P is the unique element $F \in \mathbb{Z}_p[\![x]\!]$ satisfying $F(0) = 0$ and $P(x,F) = 0$.

The condition $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$ says that the coefficient of x^0y^1 in P is nonzero modulo p and implies that $\deg_y(P \bmod p) \geq 1$. If $\deg_x P = 0$, then F is the trivial 0 series; we exclude it since otherwise the statement of the following theorem does not hold when $h = 0$.

Theorem 1. *Let p be a prime, let $\alpha \geq 1$, and let $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!] \setminus \{0\}$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$. Let $h := \deg_x(P \bmod p)$ and $d := \deg_y(P \bmod p)$, and assume $h = \deg_x P$ and $d = \deg_y P$. Then the size of the minimal p-automaton generating $(a(n) \bmod p^\alpha)_{n\geq 0}$ is in*

$$(1 + o(1))\, p^{\frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha+hd+1)}$$

as any of p, α, h, or d tends to infinity and the others remain constant.

Theorem 1 follows from a finer result, whose statement involves the following functions. Define $\mathrm{parts}(n)$ to be the set of all integer partitions of n. The *Landau function* $g(n)$ is the maximum value of $\mathrm{lcm}(\sigma)$ over all integer partitions $\sigma \in \mathrm{parts}(n)$ [20, A000793]. For example, $g(5)$ is the maximum value among $\mathrm{lcm}(5)$, $\mathrm{lcm}(4,1)$, $\mathrm{lcm}(3,2)$, $\mathrm{lcm}(3,1,1)$, $\mathrm{lcm}(2,2,1)$, $\mathrm{lcm}(2,1,1,1)$, and $\mathrm{lcm}(1,1,1,1,1)$, so $g(5) = 6$. Finally, define

$$\mathcal{L}(l,m,n) := \max_{\substack{1\leq i\leq l \\ 1\leq j\leq m \\ 1\leq k\leq n}} \max_{\substack{\sigma_1\in\mathrm{parts}(i) \\ \sigma_2\in\mathrm{parts}(j) \\ \sigma_3\in\mathrm{parts}(k)}} \mathrm{lcm}(\mathrm{lcm}(\sigma_1), \mathrm{lcm}(\sigma_2), \mathrm{lcm}(\sigma_3)).$$

In the following theorem, we remove the mild conditions $h = \deg_x P$ and $d = \deg_y P$. They are needed in Theorem 1 for the asymptotic result, since otherwise a family of polynomials P can be chosen such that $\deg_x P = p^{p^h}$ or $\deg_y P = p^{p^d}$, and for such families the value of p^u in Theorem 2 grows too quickly as h or d gets large. Note that the conditions of Theorem 1 imply $u = 1$. The maps $\pi_{x,i}$ and $\pi_{y,j}$ project bivariate Laurent polynomials to univariate Laurent polynomials; for the definitions, see Section 5.

Theorem 2. *Let p be a prime, let $\alpha \geq 1$, and let $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!]$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$ such that $h := \deg_x(P \bmod p) \geq 1$. Let $d = \deg_y(P \bmod p)$,*

$$N = \tfrac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd + 1),$$

and

$$u = \left\lfloor \log_p \max\big(\alpha(\deg_x(P \bmod p^\alpha) - h), \alpha(\deg_y(P \bmod p^\alpha) - d) + 1\big) \right\rfloor + 1.$$

Let $Q \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ be a lift of $P/y \bmod p$ which has the same monomial support as $P/y \bmod p$, and let

$$\begin{aligned} u_\ell &= \left\lfloor \log_p \max\big(p^{\alpha-1}(d - 1 - \deg \pi_{x,0}(Q)), 1\big) \right\rfloor + 1 \\ u_{\mathrm{r}} &= \left\lfloor \log_p \max\big(p^{\alpha-1}(d - 1 - \deg \pi_{x,h}(Q)), 1\big) \right\rfloor + 1 \\ u_{\mathrm{t}} &= \left\lfloor \log_p \max\big(p^{\alpha-1}(h - \deg \pi_{y,d-1}(Q)), 1\big) \right\rfloor + 1. \end{aligned}$$

Then the minimal p-automaton that generates $(a(n) \bmod p^\alpha)_{n\geq 0}$ has size at most

$$p^N + p^{N-\alpha(\alpha+1)(h+d-1)/2}\mathcal{L}(h,d,d) + \max(u_\ell, u_\mathrm{r}, u_\mathrm{t}) + \left\lceil \log_p \max(h, d-1) \right\rceil + \max(\alpha, 2(\alpha-1)) + \tfrac{p^u-1}{p-1}.$$

We can recover the bound for a sequence of elements in the field $\mathbb{F}_p$ [16, Theorem 1] as follows. Let $\alpha = 1$, and let $P \in \mathbb{F}_p[x,y]$ such that $\deg_x P = h$ and $\deg_y P = d$, so that $u = 1$. Then the bound in Theorem 2 is at most

$$p^{hd} + p^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \left\lfloor \log_p \max(h, d-1) \right\rfloor + 1 + \left\lceil \log_p \max(h, d-1) \right\rceil + 1 + 1.$$

When we use the further specificity of working over a field, one obtains the bound

$$p^{hd} + p^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \left\lfloor \log_p h \right\rfloor + \left\lceil \log_p \max(h, d-1) \right\rceil + 3 \tag{1}$$

in the previous article [16].

Explicit computations suggest that the bound (1) for sequences of elements in $\mathbb{F}_p$ is asymptotically sharp but that the bound in Theorem 2 is not. The appendix of this article contains the results of searches for large automata for comparison. Bounds on the automaton size have implications for the time complexity of any algorithm that computes an automaton generating $(a(n) \bmod p^\alpha)_{n\geq 0}$. In particular, the algorithm we describe in Section 2 has been used to systematically answer number theoretic questions about sequences arising in combinatorics and number theory, such as the Catalan numbers and Apéry numbers [17]. We mention that another approach to this same question, using sequences represented as constant terms of powers of Laurent polynomials rather than diagonals of rational functions, has also been quite successful [19, 11, 21, 3].

The main innovation in this article is a new numeration system for a family of bivariate Laurent polynomials. This numeration system behaves in many ways like base-p representations of integers, except that the digits are Laurent polynomials whose degrees can increase from one digit to the next. States of the automaton for $(a(n) \bmod p^\alpha)_{n\geq 0}$ are identified with bivariate Laurent polynomials, as in Section 2, and we show that each state has a unique base-$\frac{p}{Q}$ representation, as defined in Section 3, consisting of α digits. Most Laurent polynomials are not representable in this numeration system and therefore do not represent states. This allows us to avoid a doubly exponential upper bound on the number of states. By bounding the degrees of the digits, we obtain the bound in Theorem 2.

There are other benefits of base-$\frac{p}{Q}$ representations as well. Representations of states in this numeration system are much more compact than their full expansions as Laurent polynomials, so using base-$\frac{p}{Q}$ representations greatly the reduces the amount of memory and time required to compute an automaton. For the sequence of Catalan numbers $C(n)_{n\geq 0}$, previously we were able to compute an automaton for $(C(n) \bmod 2^9)_{n\geq 0}$, which has 2403 states, but not for larger powers of 2 [17]. With base-$\frac{p}{Q}$ representations, we are able to compute an automaton for $(C(n) \bmod 2^{14})_{n\geq 0}$; it has 174037 states and required 34GB of memory. From this automaton, one computes that only $\frac{2990}{2^{14}} \approx 18.2\%$ of the residues modulo 2^{14} are attained by the Catalan numbers, and only $\frac{2037}{2^{14}} \approx 12.4\%$ of residues are attained infinitely many times. This establishes the new upper bound of 0.124 on the density of the set $\{C(n) : n \geq 0\}$ in $\mathbb{Z}_2$. It is not known whether this density is positive.

We prove Theorem 2 in three steps. The first step is carried out in Section 3, where we describe the base-$\frac{p}{Q}$ numeration system. This first step is not present in

the proof of the bound (1), since when $\alpha = 1$ the base-$\frac{p}{Q}$ representation consists only of a single digit and does not place any restrictions on Laurent polynomials that represent states.

The second step is to obtain a preliminary upper bound on the automaton size. This is the subject of Section 4. We define a vector space $\mathcal{W}$ and show that $\mathcal{W}$ contains the base-$\frac{p}{Q}$ representations of most of the automaton states. To do this, we bound the degrees of the digits of the base-$\frac{p}{Q}$ representations of states. The space $\mathcal{W}$ has dimension $N = \frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd + 1)$, and this gives the main term in Theorem 2. The only states whose base-$\frac{p}{Q}$ representations do not belong to $\mathcal{W}$ are those reachable from the initial state by either a fixed small number of transitions or reading a sequence of 0s. The former are counted easily, and the latter correspond to the states in the orbit of the initial state under a certain linear transformation $\lambda_{0,0}$.

The third and longest step in the proof of Theorem 2 is to bound the orbit size of the initial state under $\lambda_{0,0}$. We do this by studying the structure of $\lambda_{0,0}$ as a linear transformation on bivariate Laurent polynomials. We essentially decompose the space containing the automaton states into four subspaces — three "borders" and an "interior". On the interior, we have no control over the behavior of $\lambda_{0,0}$ except what we get from base-$\frac{p}{Q}$ representations. On the three borders, however, we have significant control. In Section 5, we show that $\lambda_{0,0}$, when restricted to each of the borders, behaves like a linear transformation λ_0 on univariate Laurent polynomials. This is analogous to part of the proof of the bound (1), but here we must also show that the base-$\frac{p}{Q}$ representations are compatible. Next, we must bound orbit sizes under λ_0. We do this by first bounding the period length of the coefficient sequence of a univariate rational power series of the form $\frac{1}{R^{p^{\alpha-1}}} \bmod p^\alpha$ in Section 6. We use results of Engstrom [9] that bound period lengths of coefficient sequences of rational series modulo p and modulo p^α. Then, in Section 7, we transfer the bound on the period length of $\frac{1}{R^{p^{\alpha-1}}} \bmod p^\alpha$ to a bound on the orbit size of a univariate Laurent polynomial under λ_0. In Section 8, we complete the proof of Theorem 2 by showing how the orbit sizes under λ_0 contribute to the orbit size under $\lambda_{0,0}$. Theorem 1 follows relatively easily.

Bounding the period lengths of coefficients of rational power series in Section 6 and the orbit size under λ_0 in Section 7 are considerably more involved over $\mathcal{R}_{p^\alpha}$ than in the proof of (1), which relied on facts about finite fields. One difficulty is that $\mathcal{R}_{p^\alpha}[z]$ does not have unique factorization. Fortunately, the first bound essentially depends on the period length of the coefficient sequence modulo p. Also, we use a lifting-the-exponent lemma throughout to show that the second bound essentially depends on information modulo p.

In Section 9, we generalize from algebraic series to diagonals of rational functions. The proof of Theorem 2 begins by converting the algebraic power series F to the diagonal of a rational function in 2 variables. By starting directly with the latter, the same approach allows us to bound the automaton size for the diagonal of a rational function in m variables modulo p^α, where the diagonal operator $\mathcal{D}$ is defined on multivariate series analogously to bivariate series.

Theorem 3. *Let p be a prime, let $\alpha \geq 1$, and let*

$$F := \mathcal{D}\left(\frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)}\right)$$

where $P(x_1, \ldots, x_m)$ *and* $Q(x_1, \ldots, x_m)$ *are polynomials in* $\mathbb{Z}_p[x_1, \ldots, x_m]$ *such that* $Q(0, \ldots, 0) \not\equiv 0 \mod p$ *and* $m \geq 2$. *Write* $F = \sum_{n \geq 0} a(n)x^n$. *Let* $h_i = \max(\deg_{x_i}(P \bmod p), \deg_{x_i}(Q \bmod p))$, *and assume that* $h_i \geq 1$ *for each* i. *Let* $M = \sum_{k=0}^{\alpha-1} \prod_{i=1}^{m}((k+1)h_i + 1)$. *Then the minimal* p*-automaton that generates* $(a(n) \bmod p^\alpha)_{n \geq 0}$ *has size at most* p^M.

The dominant factor in the previous bound is $p^{\alpha^{m+1}h_1 \cdots h_m}$. When $m = 2$, we refine Theorem 3 to obtain an asymptotic bound in Theorem 46; however, this approach does not currently extend to $m \geq 3$. When $\alpha = 1$, the dimension in Theorem 3 is $M = \prod_{i=1}^{m}(h_i + 1)$. Adamczewski, Bostan, and Caruso [1, Corollary 1.4] previously obtained this bound for multivariate algebraic series F, with a further refinement involving the total height of the annihilating polynomial of F.

Finally, in Section 10, we give another application of the base-$\frac{p}{Q}$ numeration system. For a given algebraic power series F, the automaton for $F \bmod p^\alpha$ projects naturally to the automaton for $F \bmod p^\beta$ for each $\beta \leq \alpha$, as was shown by the authors [18]. Consequently, the inverse limit as $\alpha \to \infty$ of these automata exists. However, no explicit description of its states was known. We show that the base-$\frac{p}{Q}$ representations of the states of the automaton for $F \bmod p^\beta$ are simply truncations of those for $F \bmod p^\alpha$. This gives explicit descriptions of the states of the inverse limit automaton as inverse limits of finite base-$\frac{p}{Q}$ representations.

2. The module of possible states

In this section, we recall the construction of the automaton generating $(a(n) \bmod p^\alpha)_{n \geq 0}$, where p is a prime and $\alpha \geq 1$. We assume the reader is familiar with deterministic finite automata with output; see [2] for a comprehensive treatment and [15] for a short introduction. An automaton with input alphabet $\{0, 1, \ldots, p-1\}$ generates the p-automatic sequence whose nth term is the output of the automaton when fed the standard base-p representation of n, starting with the least significant digit.

Theorems 1 and 2 are concerned with automatic sequences with elements in $\mathcal{R}_{p^\alpha}$. These sequences arise in the following result of Denef and Lipshitz [8, Lemma 6.3], which extends Furstenberg's theorem [10] to an integral domain. We state it for the p-adic integers, along with an automaticity result proved by Denef and Lipshitz [8, Remark 6.6]; see also [17, Theorem 2.1]. The *diagonal operator* $\mathcal{D}$, acting on bivariate power series, is defined by

$$\mathcal{D}\left(\sum_{m \geq 0}\sum_{n \geq 0} a(m,n)x^m y^n\right) = \sum_{n \geq 0} a(n,n)x^n.$$

Theorem 4 (Denef and Lipshitz)**.** *Let* p *be a prime. Let* $P \in \mathbb{Z}_p[x, y]$ *such that* $P(0,0) = 0$ *and* $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$. *Let* F *be the Furstenberg series associated with* P. *Then*

$$F = \mathcal{D}\left(\frac{y\frac{\partial P}{\partial y}(xy, y)}{P(xy, y)/y}\right).$$

Moreover, for each $\alpha \geq 1$, *the coefficient sequence of* $F \bmod p^\alpha$ *is* p*-automatic.*

Since we will be working modulo p^α, we are mostly interested in sequences $a(n)_{n \geq 0}$ with entries from the set $\mathcal{R}_{p^\alpha}$. We establish a correspondence between

states of an automaton and Laurent polynomials in $\mathcal{R}_{p^\alpha}[x, y, y^{-1}]$. We do this by identifying states first with sequences and then with power series. Finally, Theorem 4 will allow us to identify automaton states with Laurent polynomials. To do this we will use the *p-kernel* of $a(n)_{n\geq 0}$, defined as

$$\ker_p(a(n)_{n\geq 0}) := \{a(p^e n + r)_{n\geq 0} : e \geq 0 \text{ and } 0 \leq r \leq p^e - 1\}.$$

The smallest automaton that generates $a(n)_{n\geq 0}$ and that is not affected by leading 0s is its *minimal automaton*. Eilenberg's theorem gives a bijection between the states of the minimal automaton and the elements of the p-kernel.

We represent kernel sequences $a(p^e n+r)_{n\geq 0}$ by their generating series $\sum_{n\geq 0} a(p^e n+r)x^n$. Elements of the p-kernel can be accessed by applying the following operators.

Definition. Let $n \in \mathbb{Z}$. For each $r \in \{0, 1, \ldots, p-1\}$, define the *Cartier operator* Λ_r on the monomial x^n by

$$\Lambda_r(x^n) = \begin{cases} x^{\frac{n-r}{p}} & \text{if } n \equiv r \mod p \\ 0 & \text{otherwise.} \end{cases}$$

Then extend Λ_r linearly to polynomials, Laurent polynomials, and Laurent series in x with coefficients in $\mathcal{R}_{p^\alpha}$. In particular, for polynomials we have

$$\Lambda_r\left(\sum_{n=0}^{N} a(n)x^n\right) = \sum_{n=0}^{\lfloor N/p \rfloor} a(pn+r)x^n.$$

Similarly, for $m, n \in \mathbb{Z}$ and $r, s \in \{0, 1, \ldots, p-1\}$, define the bivariate Cartier operator

$$\Lambda_{r,s}(x^m y^n) = \begin{cases} x^{\frac{m-r}{p}} y^{\frac{n-s}{p}} & \text{if } m \equiv r \mod p \text{ and } n \equiv s \mod p \\ 0 & \text{otherwise,} \end{cases}$$

and extend $\Lambda_{r,s}$ linearly to bivariate polynomials, Laurent polynomials, and Laurent series.

The operator Λ_r has the following useful property.

Proposition 5. *Let p be a prime, let $\alpha \geq 1$, and let $r, s \in \{0, 1, \ldots, p-1\}$. For all univariate Laurent series F and G with coefficients in $\mathcal{R}_{p^\alpha}$, we have $\Lambda_r(GF^{p^\alpha}) = \Lambda_r(G)F^{p^{\alpha-1}}$. Similarly, for all bivariate Laurent series F and G with coefficients in $\mathcal{R}_{p^\alpha}$, we have $\Lambda_{r,s}(GF^{p^\alpha}) = \Lambda_{r,s}(G)F^{p^{\alpha-1}}$.*

A proof of Proposition 5 can be found in [17, Proposition 1.9]. It uses the following lifting-the-exponent lemma for (Laurent) polynomials, whose proof is analogous to the proof for integers. We will use Lemma 6 throughout this article.

Lemma 6. *If $R, \bar{R} \in \mathbb{Z}_p[x, x^{-1}]$ and $R \equiv \bar{R} \mod p$, then $R^{p^{\alpha-1}} \equiv \bar{R}^{p^{\alpha-1}} \mod p^\alpha$. Similarly, if $Q, \bar{Q} \in \mathbb{Z}_p[x, x^{-1}, y, y^{-1}]$ and $Q \equiv \bar{Q} \mod p$, then $Q^{p^{\alpha-1}} \equiv \bar{Q}^{p^{\alpha-1}} \mod p^\alpha$.*

The final step is to establish a connection between a power series $\sum_{n\geq 0} a(p^e n + r)x^n$ corresponding to a kernel sequence and a Laurent polynomial. This Laurent polynomial will be the numerator of a rational function whose diagonal is the desired power series. We do this using Theorem 4. We shear bivariate series by replacing

x with xy^{-1}. When we do this, the diagonal operator is replaced by the *center row operator* $\mathcal{C}$, defined by

$$\mathcal{C}\left(\sum_{m\geq 0}\sum_{n\in\mathbb{Z}} a(m,n)x^m y^n\right) = \sum_{m\geq 0} a(m,0)x^m.$$

We have

$$\Lambda_r\mathcal{C}\left(\frac{S}{Q^{p^{\alpha-1}}}\right) = \mathcal{C}\Lambda_{r,0}\left(\frac{S}{Q^{p^{\alpha-1}}}\right) = \mathcal{C}\Lambda_{r,0}\left(\frac{SQ^{p^\alpha-p^{\alpha-1}}}{Q^{p^\alpha}}\right) = \mathcal{C}\left(\frac{\Lambda_{r,0}\left(SQ^{p^\alpha-p^{\alpha-1}}\right)}{Q^{p^{\alpha-1}}}\right),$$

where the last equality follows from Proposition 5. Note that the initial and final series in this equation have the same denominator $Q^{p^{\alpha-1}}$. Therefore the map $S \mapsto \Lambda_{r,0}\left(SQ^{p^\alpha-p^{\alpha-1}}\right)$ on $\mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ emulates the Cartier operator Λ_r on $\mathcal{R}_{p^\alpha}[\![x]\!]$. We will represent states of the automaton by Laurent polynomials $S \in \mathcal{R}_{p^\alpha}[x,y,y^{-1}]$. The main reason for shearing is that it separates the contributions of h and d; otherwise, in Proposition 20 below, the y-degree would be bounded by a function of $h+d$ rather than just of d.

This final step of converting a power series to a Laurent polynomial is not bijective. This is because different rational functions can have the same diagonal. Therefore the automaton we will construct is not necessarily minimal.

We introduce notation for the initial state of the automaton and the emulating map as follows.

Notation. Let p be prime and $\alpha \geq 1$. Let $P \in \mathbb{Z}_p[x,y]$ be a polynomial such that $P(0,0) = 0$ and $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$. Define $h := \deg_x(P \bmod p)$ and $d := \deg_y(P \bmod p)$. The Furstenberg series F given by Theorem 4 has coefficients in $\mathbb{Z}_p$. We define a Laurent polynomial Q as follows. Take $P/y \bmod p$, and let $Q \in \mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ be a lift of $P/y \bmod p$ which has the same monomial support as $P/y \bmod p$; in particular $\deg_x Q = h$ and $\deg_y Q = d-1$. For example, an element of $\mathcal{R}_p[x,y,y^{-1}]$ can be lifted in a standard way to $\mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ by identifying $\mathcal{R}_p$ with $D = \{0,1,\ldots,p-1\}$. This somewhat convoluted definition of Q allows us obtain optimal bounds even in the situation that the x- or y-degree of $P/y \bmod p$ is less than that of $P/y \bmod p^\alpha$; if neither degree drops, then one can simply take Q to be $P/y \bmod p^\alpha$. We define an automaton whose initial state is

$$S_0 := \left(y\tfrac{\partial P}{\partial y}\,(P/y)^{p^{\alpha-1}-1} \bmod p^\alpha\right).$$

For each $r \in \{0,1,\ldots,p-1\}$, define $\lambda_{r,0}\colon \mathcal{R}_{p^\alpha}[x,y,y^{-1}] \to \mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ by

$$\lambda_{r,0}(S) := \Lambda_{r,0}\left(SQ^{p^\alpha-p^{\alpha-1}}\right). \tag{2}$$

Define $\mathcal{M}_{p^\alpha}$ to be the smallest subset of $\mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ that contains S_0 and is closed under the operators $\lambda_{r,0}$. The operators $\lambda_{r,0}$ define the transitions between states. Finally, the output associated with the state $S \in \mathcal{M}_{p^\alpha}$ is the constant term of S divided by the constant term of $Q^{p^{\alpha-1}}$.

Remark 7. The condition $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$ implies $d \geq 1$. Furthermore, if $F \bmod p^\alpha$ is not a polynomial then $h \geq 1$. This is because $h = 0$ implies that the coefficient of each monomial $x^i y^j$ in P with $i \geq 1$ is 0 modulo p. Therefore the denominator $P(xy,y)/y$ in Theorem 4 also has this property. Using the geometric

series formula to expand the rational expression, we obtain a bivariate series that contains only finitely many nonzero diagonal monomials modulo p^α.

Note that, a priori, the operator $\lambda_{r,0}$ in Equation (2) should be defined with $P/y \bmod p^\alpha$ in place of Q. However, Lemma 6 gives us the following.

Proposition 8. *For all $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ and for each $r \in \{0, 1, \ldots, p-1\}$, we have*

$$\Lambda_{r,0}\Big(S(P/y \bmod p^\alpha)^{p^\alpha - p^{\alpha-1}}\Big) = \Lambda_{r,0}\Big(SQ^{p^\alpha - p^{\alpha-1}}\Big) = \lambda_{r,0}(S).$$

We will use the following elementary lemma.

Lemma 9. *The set of bivariate Laurent polynomials with the property that every nonzero monomial $c\,x^I y^J$ satisfies $J \geq -I$ is closed under addition, multiplication, and each Cartier operator $\Lambda_{r,0}$.*

Proposition 10. *The constructed automaton is not sensitive to leading* 0*s.*

Proof. Let $S \in \mathcal{M}_{p^\alpha}$, let $x^i y^j$ be a stripped monomial in S (that is, a monomial without its coefficient), and let $x^I y^J$ be a stripped monomial in $Q^{p^\alpha - p^{\alpha-1}}$; we are interested in products $x^i y^j \cdot x^I y^J$ which equal 1, since these contribute to the constant term and therefore the output value. This implies $I = -i$ and $J = -j$. Since $i \geq 0$ and $I \geq 0$, we have $i = 0 = -I$. We consider the three cases $j < 0$, $j > 0$, and $j = 0$. If $j > 0$, then $J < 0$; this implies $I > 0$ by the condition $P(0,0) \neq 0$, which contradicts $I = 0$. If $j < 0$, then $-i \leq j < 0$ by Lemma 9, which implies $i < 0$ and contradicts $i = 0$. Therefore $j = 0 = J$, so the constant term of $SQ^{p^\alpha - p^{\alpha-1}}$ is the product of the constant term of S and the constant term of $Q^{p^\alpha - p^{\alpha-1}}$. The assumption $\frac{\partial P}{\partial y}(0,0) \not\equiv 0 \mod p$ implies that the constant term $c\,x^0 y^0$ of Q is nonzero modulo p. It follows that the constant term of $Q^{p^\alpha - p^{\alpha-1}}$ is $c^{p^\alpha - p^{\alpha-1}} = 1$, since the Euler totient function satisfies $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Therefore the constant term of $\lambda_{0,0}(S)$ divided by the constant term of Q, which is the output assigned to the state $\lambda_{0,0}(S)$, is the constant term of S divided by the constant term of Q. □

3. A numeration system for the automaton states

In this section, we define a numeration system for a certain set of Laurent polynomials. We then show in Theorems 14 and 17 that all states of the automaton $\mathcal{M}_{p^\alpha}$ have a representation in this numeration system.

We continue to assume that p is a prime number and $\alpha \geq 1$. We also continue to use Q as defined in the previous section, although the only property we need for a numeration system is that the constant term of Q is nonzero modulo p.

Definition. Let $D = \{0, 1, \ldots, p-1\}$; we view $D \subseteq \mathcal{R}_{p^\alpha}$. We say that $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ has a *base-$\frac{p}{Q}$ representation* if there are Laurent polynomials $T_0, T_1, \ldots, T_{\alpha-1}$ such that $T_k \in D[x, y, y^{-1}]$ for each k and

$$S = \Big(T_0 + T_1\,\tfrac{p}{Q} + T_2\,(\tfrac{p}{Q})^2 + \cdots + T_{\alpha-1}\,(\tfrac{p}{Q})^{\alpha-1}\Big)\,Q^{p^{\alpha-1}-1}. \tag{3}$$

We refer to $T_0, T_1, \ldots, T_{\alpha-1}$ as *digits*. Since $p^{\alpha-1} - 1 \geq \alpha - 1$, the right side of Equation (3) is a Laurent polynomial.

Because of the factor $Q^{p^{\alpha-1}-1}$, this numeration system is not exactly analogous to classical base-p representations of integers. In addition, the set of possible digits is currently infinite; later we will restrict it. We start by showing that, like classical numeration systems, base-$\frac{p}{Q}$ representations have two desirable properties.

Proposition 11. *If the Laurent polynomial $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ has a base-$\frac{p}{Q}$ representation, then this representation is unique.*

Proof. Suppose that

$$\begin{aligned}(4)\quad &\left(T_0 + T_1 \tfrac{p}{Q} + \cdots + T_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1} \\ &\qquad \equiv \left(U_0 + U_1 \tfrac{p}{Q} + \cdots + U_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1} \mod p^\alpha,\end{aligned}$$

where the digits T_k and U_k belong to $D[x, y, y^{-1}]$. Then $T_0 Q^{p^{\alpha-1}-1} \equiv U_0 Q^{p^{\alpha-1}-1} \mod p$. Since Q has a constant term which is nonzero modulo p, it is invertible, so $T_0 \equiv U_0 \mod p$, which implies $T_0 = U_0$. Inductively, suppose that $T_m = U_m$ for $0 \le m \le k-1$. Reducing Equation (4) modulo p^{k+1} and expanding gives us

$$\begin{aligned}&T_0 Q^{p^{\alpha-1}-1} + \cdots + T_k p^k Q^{p^{\alpha-1}-k-1} \\ &\qquad \equiv U_0 Q^{p^{\alpha-1}-1} + \cdots + U_k p^k Q^{p^{\alpha-1}-k-1} \mod p^{k+1}.\end{aligned}$$

Subtracting the first k terms from both sides and dividing by $Q^{p^{\alpha-1}-k-1}$, we conclude that $T_k = U_k$. □

The next proposition allows us to perform carries and therefore normalize base-$\frac{p}{Q}$ representations where the digit coefficients are not in D. This implies that the set of Laurent polynomials with base-$\frac{p}{Q}$ representations is closed under addition and scalar multiplication; we will use this vector space structure in later sections.

Proposition 12. *Suppose $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ is of the form*

$$\left(T'_0 + T'_1 \tfrac{p}{Q} + T'_2 (\tfrac{p}{Q})^2 + \cdots + T'_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1}$$

where $T'_k \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ for each $k \in \{0, 1, \ldots, \alpha-1\}$. Then S has a base-$\frac{p}{Q}$ representation.

Proof. To put S into the desired form, so that it has a representation with digits $T_k \in D[x, y, y^{-1}]$, it is sufficient to show how to perform a carry from one digit to the next. We begin the procedure by setting $T''_0 = T'_0$. Given T''_k, we perform division to write it as $T''_k = pU_k + R_k$ with $R_k \in D[x, y, y^{-1}]$. Then

$$\begin{aligned}S &= \left(T_0 + \cdots + (R_k + pU_k) (\tfrac{p}{Q})^k + T'_{k+1} (\tfrac{p}{Q})^{k+1} + \cdots + T'_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1} \\ &= \left(T_0 + \cdots + R_k (\tfrac{p}{Q})^k + (U_k Q + T'_{k+1}) (\tfrac{p}{Q})^{k+1} + \cdots + T'_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1},\end{aligned}$$

so that we can set $T_k = R_k$. □

Notation. If S has a base-$\frac{p}{Q}$ representation, then S can be written uniquely as $S = \left(\sum_{k=0}^{\alpha-1} T_k (\frac{p}{Q})^k\right) Q^{p^{\alpha-1}-1}$ by Proposition 11. Define

$$(5)\qquad \operatorname{rep}_{p/Q}(S) := (T_{\alpha-1}, \ldots, T_1, T_0).$$

Let $\mathrm{dig}_k(S)$ denote the kth digit T_k in $\mathrm{rep}_{p/Q}(S)$. Finally, define

$$\mathrm{val}_{p/Q}((T_{\alpha-1},\dots,T_1,T_0)) := \left(\sum_{k=0}^{\alpha-1} T_k\,(\tfrac{p}{Q})^k\right) Q^{p^{\alpha-1}-1}.$$

Example 13. Let $P = xy^2+(x+1)y+x$. The coefficient sequence $a(n)_{n\geq 0}$ of the Furstenberg series F satisfying $P(x,F)=0$ is $0,-1,1,-2,4,-9,21,-51,\dots$ and is a signed, shifted variant of the sequence of Motzkin numbers [20, A001006]. Let $p=2$ and $\alpha=3$. Consider the initial state $S_0 \in \mathcal{R}_8[x,y,y^{-1}]$ of the automaton generating $(a(n) \bmod 8)_{n\geq 0}$. By definition,

$$\begin{aligned} S_0 = \left(y\tfrac{\partial P}{\partial y}\,(P/y)^3 \bmod 8\right) &= 2x^4y^5 + \left(7x^4+7x^3\right)y^4 + \left(7x^4+2x^3+x^2\right)y^3 \\ &+ \left(4x^4+6x^3+7x^2+5x\right)y^2 + \left(3x^4+4x^3+2x^2+4x+1\right)y \\ &+ \left(4x^4+2x^3+x^2+3x\right) + \left(5x^4+6x^3+3x^2\right)y^{-1} + \left(x^4+x^3\right)y^{-2}. \end{aligned}$$

By Theorem 17, which we state below, the initial state has a base-$\frac{p}{Q}$ representation, where $Q = xy+(x+1)+xy^{-1} \in \mathcal{R}_8[x,y,y^{-1}]$, namely

$$S_0 = \left((x+1)y + \left(x^2y^3+(x^2+x)y^2+x^2y\right)\tfrac{2}{Q} + 0\cdot\tfrac{4}{Q^2}\right)Q^3,$$

so that

$$\mathrm{rep}_{2/Q}(S_0) = \left(0,\, x^2y^3+(x^2+x)y^2+x^2y,\, (x+1)y\right).$$

Theorem 14. *The set of Laurent polynomials in $\mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ with a base-$\frac{p}{Q}$ representation is closed under $\lambda_{r,0}$ for $0\leq r\leq p-1$.*

The proof uses Lemma 15 below. For a Laurent polynomial $S \in \mathcal{R}_{p^\alpha}[x,y,y^{-1}]$, let $\mathrm{mindeg}_y S$ be the smallest y-degree of a monomial in S with a nonzero coefficient. If $\beta=1$, then the statement of Lemma 15 follows from Proposition 5, since, modulo p, we have $\Lambda_{r,0}(\frac{T}{Q^{k+1}})Q^{k+1} \equiv \Lambda_{r,0}(\frac{TQ^{p(k+1)}}{Q^{k+1}}) = \Lambda_{r,0}(TQ^{(p-1)(k+1)})$, and the latter is a Laurent polynomial; it can be verified that it satisfies the claimed degree bounds.

Lemma 15. *Let $\beta \in \{1,2,\dots,\alpha\}$, $T \in \mathcal{R}_{p^\beta}[x,y,y^{-1}]$, and $r\in\{0,1,\dots,p-1\}$. For all $k\geq 0$, the Laurent series $S := \Lambda_{r,0}(\frac{T}{(Q \bmod p^\beta)^{k+1}})(Q \bmod p^\beta)^{k+\beta}$ is a Laurent polynomial. Moreover, its degrees satisfy*

$$\begin{aligned} \deg_x S &\leq (k+\beta)h + \left\lfloor \tfrac{\deg_x T-(k+1)h-r}{p} \right\rfloor \\ \deg_y S &\leq (k+\beta)(d-1) + \left\lfloor \tfrac{\deg_y T-(k+1)(d-1)}{p} \right\rfloor \\ \mathrm{mindeg}_y S &\geq -(k+\beta) + \left\lceil \tfrac{\mathrm{mindeg}_y T+(k+1)}{p} \right\rceil. \end{aligned}$$

Finally, if each nonzero monomial $c\,x^Iy^J$ in T satisfies $J\geq -I$, then so does each nonzero monomial in S.

Proof. For ease of notation, in this proof we use Q to refer to $Q \bmod p^\beta$. Since $Q(x^p,y^p) \equiv Q(x,y)^p \mod p$, we have $\Delta := Q(x^p,y^p)-Q(x,y)^p \equiv 0 \mod p$. Therefore

$$\frac{Q(x^p,y^p)^{k+\beta}}{Q^{k+1}} = \frac{(Q^p+\Delta)^{k+\beta}}{Q^{k+1}} = \sum_{m=0}^{k+\beta}\binom{k+\beta}{m}Q^{pm-k-1}\Delta^{k+\beta-m}.$$

For $m \in \{0, 1, \ldots, k\}$, the summand is 0 since $\Delta^\beta = 0$. Therefore

$$\frac{Q(x^p, y^p)^{k+\beta}}{Q^{k+1}} = \sum_{m=k+1}^{k+\beta} \binom{k+\beta}{m} Q^{pm-k-1} \Delta^{k+\beta-m} =: Z. \tag{6}$$

This Laurent series Z is a Laurent polynomial since, for all $m \geq k+1$, we have $pm - k - 1 \geq p(k+1) - k - 1 \geq 0$. Let $z \in \{x, y\}$. Since $\deg_z \Delta \leq p \deg_z Q$, the degree of $Q^{pm-k-1}\Delta^{k+\beta-m}$ is at most $((k+\beta)p - k - 1)\deg_z Q$, so this is also an upper bound on $\deg_z Z$. Analogously, $\operatorname{mindeg}_y Z \geq ((k+\beta)p - k - 1)\operatorname{mindeg}_y Q \geq -((k+\beta)p - k - 1)$.

Multiplying both sides by T, we have $\frac{TQ(x^p,y^p)^{k+\beta}}{Q^{k+1}} = TZ$. Since the Laurent polynomial $Q(x^p, y^p)^{k+\beta}$ consists of terms with exponents that are multiples of p, applying $\Lambda_{r,0}$ to both sides gives $\Lambda_{r,0}(\frac{T}{Q^{k+1}})Q^{k+\beta} = \Lambda_{r,0}(TZ)$. In particular, $\Lambda_{r,0}(\frac{T}{Q^{k+1}})Q^{k+\beta}$ is a Laurent polynomial. Moreover, its z-degree and y-mindegree are as claimed, using the bounds in the previous paragraph on $\deg_z Z$ and $\operatorname{mindeg}_y Z$. Finally, since the coefficient of x^0y^{-1} in Q is 0, it follows from Lemma 9 that each nonzero monomial $c\,x^I y^J$ in Δ and Z satisfies $J \geq -I$. Therefore if each nonzero monomial in T also satisfies this constraint, then, again by Lemma 9, so does each nonzero monomial in S. □

We can now establish closure under $\lambda_{r,0}$.

Proof of Theorem 14. Let S be a Laurent polynomial with a base-$\frac{p}{Q}$ representation, and let $\operatorname{rep}_{p/Q}(S) = (T_{\alpha-1}, \ldots, T_1, T_0)$, so that

$$S = \left(T_0 + T_1 \tfrac{p}{Q} + T_2 (\tfrac{p}{Q})^2 + \cdots + T_{\alpha-1} (\tfrac{p}{Q})^{\alpha-1}\right) Q^{p^{\alpha-1}-1}.$$

We show that $\lambda_{r,0}(S)$ also has this form. To do this, for each k, we construct the base-$\frac{p}{Q}$ representation of $\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^\alpha$. The digits of these representations are Laurent polynomials $U_{k,j} \in D[x, y, y^{-1}]$, and we will recombine these Laurent polynomials to obtain the base-$\frac{p}{Q}$ representation of $\lambda_{r,0}(S)$.

Let $k \in \{0, 1, \ldots, \alpha - 1\}$. We define Laurent polynomials $U_{k,j}$ as follows. Lemma 15 with $\beta = j+1$ implies that $\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+j+1} \bmod p^{j+1}$ is a Laurent polynomial for all $j \geq 0$. For each $j \in \{0, 1, \ldots, \alpha-k-1\}$, define $U_{k,j} \in D[x, y, y^{-1}]$ to be the Laurent polynomial satisfying

$$\begin{aligned}
\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+1} &\equiv U_{k,0} \mod p \\
\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+2} &\equiv U_{k,0}Q + pU_{k,1} \mod p^2 \\
\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+3} &\equiv U_{k,0}Q^2 + pU_{k,1}Q + p^2U_{k,2} \mod p^3 \\
&\vdots \\
\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{\alpha} &\equiv U_{k,0}Q^{\alpha-k-1} + pU_{k,1}Q^{\alpha-k-2} + \cdots + p^{\alpha-k-1}U_{k,\alpha-k-1} \mod p^{\alpha-k}.
\end{aligned}$$

The Laurent polynomials $U_{k,j}$ can be recursively computed using the proof of Lemma 15. Dividing the previous congruence by $Q^{\alpha-1}$, we obtain the Laurent series congruence

$$\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q \equiv \sum_{j=0}^{\alpha-k-1} \frac{U_{k,j}}{Q^{k+j}}\, p^j \mod p^{\alpha-k}. \tag{7}$$

Using Proposition 5, we have

$$\begin{aligned}\lambda_{r,0}(S) &= \lambda_{r,0}\left(\left(\sum_{k=0}^{\alpha-1} T_k\,(\tfrac{p}{Q})^k\right) Q^{p^{\alpha-1}-1}\right)\\ &= \Lambda_{r,0}\left(\left(\sum_{k=0}^{\alpha-1} T_k\,(\tfrac{p}{Q})^k\right) Q^{-1}Q^{p^{\alpha}}\right)\\ &= \Lambda_{r,0}\left(\left(\sum_{k=0}^{\alpha-1} T_k\,(\tfrac{p}{Q})^k\right) Q^{-1}\right) Q^{p^{\alpha-1}}\\ &= \left(\sum_{k=0}^{\alpha-1} \Lambda_{r,0}\big(T_kQ^{-k-1}\big)\,p^kQ\right) Q^{p^{\alpha-1}-1}.\end{aligned}$$

By Equation (7), we have

$$\begin{aligned}\lambda_{r,0}(S) &= \left(\sum_{k=0}^{\alpha-1}\sum_{j=0}^{\alpha-k-1} U_{k,j}\,\tfrac{p^{k+j}}{Q^{k+j}}\right) Q^{p^{\alpha-1}-1}\\ &= \left(\sum_{k=0}^{\alpha-1}\sum_{m=k}^{\alpha-1} U_{k,m-k}\,(\tfrac{p}{Q})^m\right) Q^{p^{\alpha-1}-1}\end{aligned}$$

after substituting $j = m-k$. Switching the order of summation gives

$$\lambda_{r,0}(S) = \left(\sum_{m=0}^{\alpha-1}\left(\sum_{k=0}^{m} U_{k,m-k}\right)(\tfrac{p}{Q})^m\right) Q^{p^{\alpha-1}-1}.$$

For each $m \in \{0,1,\ldots,\alpha-1\}$, set $T'_m = \sum_{k=0}^{m} U_{k,m-k}$. The coefficients in the Laurent polynomial T'_m do not necessarily belong to D. To obtain the base-$\frac{p}{Q}$ representation of $\lambda_{r,0}(S)$, we perform carries as in Proposition 12. □

Example 16. As in Example 13, let $P = xy^2 + (x+1)y + x$, $p = 2$, $\alpha = 3$, and $Q = xy + (x+1) + xy^{-1} \in \mathcal{R}_8[x,y,y^{-1}]$; we saw that $\mathrm{rep}_{2/Q}(S_0)$ is

$$(T_2, T_1, T_0) := \big(0,\, x^2y^3 + (x^2+x)y^2 + x^2y,\, (x+1)y\big)\,.$$

We follow the proof of Theorem 14 to compute $\mathrm{rep}_{2/Q}(\lambda_{0,0}(S_0))$. The first step is to compute $U_{0,0}, U_{0,1}, U_{0,2}, U_{1,0}, U_{1,1}, U_{2,0} \in D[x,y,y^{-1}]$. For $U_{0,0}$, we can use Proposition 5 to obtain

$$U_{0,0} \equiv \Lambda_{0,0}\big(T_0Q^{-1}\big)\,Q \equiv \Lambda_{0,0}(T_0Q) \equiv xy + x \mod 2.$$

Therefore $U_{0,0} = xy + x$. For the others, we use Lemma 15. Set

$$\Delta = Q(x^2,y^2) - Q(x,y)^2 = \big(6x^2+6x\big)\,y + \big(6x^2+6x\big) + \big(6x^2+6x\big)\,y^{-1}.$$

The Laurent polynomial $U_{0,1}$ is defined by $\Lambda_{0,0}\big(T_0Q^{-1}\big)\,Q^2 \equiv U_{0,0}Q + 2U_{0,1} \mod 4$. To compute $\Lambda_{r,0}\big(T_0Q^{-1}\big)\,Q^2$, we use the proof of Lemma 15 with $k=0$ and $\beta = 2$. Let

$$Z := \sum_{m=1}^{2} \binom{2}{m} Q^{2m-1}\Delta^{2-m} = 2Q\Delta + Q^3.$$

Then

$$\Lambda_{0,0}\big(T_0Q^{-1}\big)\,Q^2 \equiv \Lambda_{0,0}(T_0Z) \equiv x^2y^2 + \big(2x^2+x\big)\,y + \big(2x^2+x\big) + x^2y^{-1} \mod 4.$$

This implies $2U_{0,1} \equiv \Lambda_{0,0}\big(T_0Q^{-1}\big)\,Q^2 - U_{0,0}Q \equiv 0 \mod 4$, so $U_{0,1} = 0$. The remaining $U_{k,j}$ are computed analogously, and we find

$$\begin{aligned} U_{0,0} &= xy + x & U_{1,0} &= x^2y^2 + \big(x^2 + x\big)\,y + x^2 \\ U_{0,1} &= 0 & U_{1,1} &= x^3y^3 + \big(x^3 + x\big)\,y + x^3y^{-1} \\ U_{0,2} &= x^2y^2 + x^2y + x^2 + x^2y^{-1} & U_{2,0} &= 0. \end{aligned}$$

The second step is to compute the new digits $T'_m = \sum_{k=0}^{m} U_{k,m-k}$. We obtain

$$\begin{aligned} T'_0 &= U_{0,0} = xy + x \\ T'_1 &= U_{0,1} + U_{1,0} = x^2y^2 + \big(x^2 + x\big)\,y + x^2 \\ T'_2 &= U_{0,2} + U_{1,1} + U_{2,0} = x^3y^3 + x^2y^2 + \big(x^3 + x^2 + x\big)\,y + x^2 + \big(x^3 + x^2\big)\,y^{-1}. \end{aligned}$$

The third step is to perform carries to normalize the base-$\frac{2}{Q}$ representation. In this example, it happens that no carries are necessary. Therefore $\operatorname{rep}_{2/Q}(\lambda_{0,0}(S_0)) = (T'_2, T'_1, T'_0)$.

Theorem 14 gets us most of the way to the following result. Recall that $\mathcal{M}_{p^\alpha}$ is the set of states of an (unminimized) automaton that generates the sequence $(a(n) \bmod p^\alpha)_{n\geq 0}$.

Theorem 17. *Every state in $\mathcal{M}_{p^\alpha}$ has a unique base-$\frac{p}{Q}$ representation.*

To prove Theorem 17, and later Proposition 23, we will use the following lemma.

Lemma 18. *For each $k \in \{0, 1, \ldots, \alpha-1\}$, the Laurent series $S := \left(\frac{Q^{k+1}}{P/y} \bmod p^{k+1}\right)$ is a Laurent polynomial. Moreover, its degrees satisfy*

$$\begin{aligned} \deg_x S &\leq k \deg_x(P \bmod p^{k+1}) \\ \deg_y S &\leq k\,\big(\deg_y(P \bmod p^{k+1}) - 1\big) \\ \operatorname{mindeg}_y S &\geq -k. \end{aligned}$$

Proof. Fix k. Since $Q \equiv P/y \mod p$, we have $\Delta := (Q - P/y \bmod p^{k+1}) \equiv 0 \mod p$. Therefore

$$\frac{Q^{k+1}}{P/y} \equiv \frac{(P/y + \Delta)^{k+1}}{P/y} \equiv \sum_{m=0}^{k+1} \binom{k+1}{m} (P/y)^{m-1}\Delta^{k+1-m} \mod p^{k+1}.$$

For $m = 0$, the summand is 0 modulo p^{k+1} since Δ is divisible by p. Therefore $\frac{Q^{k+1}}{P/y} \bmod p^{k+1}$ is a Laurent polynomial. Finally, the degree bounds follow from the fact that $\deg_z \Delta \leq \deg_z(P/y \bmod p^{k+1})$ for $z \in \{x, y\}$, and $\operatorname{mindeg}_y \Delta \geq \operatorname{mindeg}_y(P/y \bmod p^{k+1})$. □

We now use Lemma 18 to prove Theorem 17.

Proof of Theorem 17. We show that the initial state $S_0 = \left(y\frac{\partial P}{\partial y}\,(P/y)^{p^{\alpha-1}-1} \bmod p^\alpha\right)$ has a base-$\frac{p}{Q}$ representation; the result then follows from Theorem 14 and Proposition 11. We use the convention that whenever we multiply or divide a polynomial in $\mathcal{R}_{p^k}[x, y, y^{-1}]$ by a polynomial in $\mathbb{Z}_p[x, y, y^{-1}]$, we project the latter to $\mathcal{R}_{p^k}[x, y, y^{-1}]$. Conversely, we will define the digits T_k of S_0 to be in $\mathcal{R}_p[x, y, y^{-1}]$, but then we identify $\mathcal{R}_p$ with D so that we can do arithmetic in $\mathcal{R}_{p^\alpha}$ as in Equation (3). We will use $(P/y)^{p^{\alpha-1}} \equiv Q^{p^{\alpha-1}} \mod p^\alpha$, which follows from Lemma 6.

Set $T_0 = \left(y\frac{\partial P}{\partial y} \bmod p\right)$; then $S_0 \equiv y\frac{\partial P}{\partial y}(P/y)^{p^{\alpha-1}-1} \equiv T_0 Q^{p^{\alpha-1}-1} \mod p$. To define the digit T_1, we use $0 \equiv y\frac{\partial P}{\partial y} - T_0 \equiv y\frac{\partial P}{\partial y} \cdot \frac{Q}{P/y} - T_0 \mod p$, and set

$$T_1 = \left(\frac{y\frac{\partial P}{\partial y} \cdot \frac{Q}{P/y} - T_0}{p} Q \bmod p\right).$$

We have $T_1 \in \mathcal{R}_p[x, y, y^{-1}]$ since $\frac{Q^2}{P/y} \in \mathcal{R}_{p^2}[x, y, y^{-1}]$ by Lemma 18. Then

$$y\frac{\partial P}{\partial y} \cdot \frac{Q^{p^{\alpha-1}}}{P/y} \equiv \left(T_0 + T_1\frac{p}{Q}\right) Q^{p^{\alpha-1}-1} \mod p^2,$$

so we have $S_0 \equiv y\frac{\partial P}{\partial y}(P/y)^{p^{\alpha-1}-1} \equiv \left(T_0 + T_1\frac{p}{Q}\right) Q^{p^{\alpha-1}-1} \mod p^2$. Recursively, for each $k \in \{2, \ldots, \alpha-1\}$, define the Laurent polynomial

$$T_k = \left(\frac{y\frac{\partial P}{\partial y} \cdot \frac{Q}{P/y} - T_0 - T_1\left(\frac{p}{Q}\right) - \cdots - T_{k-1}\left(\frac{p}{Q}\right)^{k-1}}{p^k} Q^k \bmod p\right).$$

By Lemma 18, we have $T_k \in \mathcal{R}_p[x, y, y^{-1}]$. Then $S_0 \equiv \left(T_0 + T_1\frac{p}{Q} + \cdots + T_k\left(\frac{p}{Q}\right)^k\right) Q^{p^{\alpha-1}-1} \mod p^{k+1}$ for each k. In particular, S_0 has a base-$\frac{p}{Q}$ representation. □

4. First bounds on the size of the automaton

By Theorem 17, every state in $\mathcal{M}_{p^\alpha}$ has a base-$\frac{p}{Q}$ representation. In this section, we bound the digits of these representations, to give preliminary bounds on the size of $\mathcal{M}_{p^\alpha}$ in Corollaries 24 and 25. To do this, we will show that the base-$\frac{p}{Q}$ representations of most states live in the spaces $\mathcal{W}$ or $\mathcal{V}$ defined below in Equations (8) and (9).

Notation. Recall $D = \{0, 1, \ldots, p-1\}$. For $k \in \{0, 1, \ldots, \alpha-1\}$, let

$$W_k := \left\{ \sum_{i=0}^{(k+1)h-1} \sum_{j=\max(-k,-i)}^{(k+1)(d-1)} c_{i,j} x^i y^j : c_{i,j} \in D \text{ for each } i, j \right\}$$

and

$$V_k := \left\{ \sum_{i=0}^{(k+1)h} \sum_{j=\max(-k,-i)}^{(k+1)(d-1)} c_{i,j} x^i y^j : c_{i,j} \in D \text{ for each } i, j \right\}.$$

Define

$$\mathcal{W} := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in W_k \text{ for each } k \in \{0, 1, \ldots, \alpha-1\}\} \tag{8}$$

$$\mathcal{V} := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in V_k \text{ for each } k \in \{0, 1, \ldots, \alpha-1\}\}. \tag{9}$$

Proposition 12 implies that $\mathcal{W}$ is a D-vector space, where the vector space addition operation is addition of the corresponding Laurent polynomials. The set of all tuples of the form $(0, \ldots, 0, x^i y^j, 0, \ldots, 0)$ with the appropriate bounds on i and j forms a basis of $\mathcal{W}$, in that every element of $\mathcal{W}$ is a unique D-linear combination of this basis. Figure 1 depicts the geometry of the monomials in $\mathcal{W}$ for a particular choice of values for p, α, h, and d.

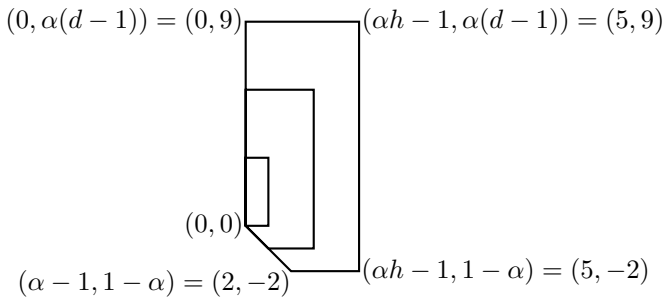

FIGURE 1. Nested polygons for $k \in \{0, 1, 2\}$ containing pairs of exponents (i, j) corresponding to monomials $x^i y^j$ in the basis of W_k, with $(p, \alpha, h, d) = (3, 3, 2, 4)$.

We compute the size N of the basis of $\mathcal{W}$ by partitioning the Newton polygon of each T_k into a rectangle and a trapezoid:

$$N := \sum_{k=0}^{\alpha-1} \left((k+1)h \cdot ((k+1)(d-1)+1) + \sum_{j=-k}^{-1} ((k+1)h + j) \right)$$

$$= \tfrac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd + 1). \tag{10}$$

Similarly, the dimension of $\mathcal{V}$ is

$$\sum_{k=0}^{\alpha-1} \left(((k+1)h+1) \cdot ((k+1)(d-1)+1) + \sum_{j=-k}^{-1} ((k+1)h + 1 + j) \right)$$

$$= \tfrac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + (h+3)d + 1). \tag{11}$$

We work with states whose base-$\frac{p}{Q}$ representation belongs to $\mathcal{V}$. For these states, one checks the following elementary result.

Lemma 19. *If $S \in \mathrm{val}_{p/Q}(\mathcal{V})$, then $\deg_x S \le p^{\alpha-1}h$, $\deg_y S \le p^{\alpha-1}(d-1)$, and $1 - p^{\alpha-1} \le \mathrm{mindeg}_y S$.*

We will see in Proposition 23 that most states belong to $\mathcal{W}$. Furthermore, in Corollary 21 we show that $\mathrm{val}_{p/Q}(\mathcal{W})$ and $\mathrm{val}_{p/Q}(\mathcal{V})$ are invariant under $\lambda_{r,0}$ for each r. To do this we use the following proposition.

Proposition 20. *Let $r \in \{0, 1, \ldots, p-1\}$, and suppose that S has a base-$\frac{p}{Q}$ representation $\mathrm{rep}_{p/Q}(S) = (T_{\alpha-1}, \ldots, T_1, T_0)$. Then the mth base-$\frac{p}{Q}$ digit T'_m of $\lambda_{r,0}(S)$ satisfies*

$$\deg_x T'_m \le \max_{0 \le k \le m} \left(\left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor \right) + (m+1)h$$

$$\deg_y T'_m \le \max_{0 \le k \le m} \left(\left\lfloor \tfrac{\deg_y T_k - (k+1)(d-1)}{p} \right\rfloor \right) + (m+1)(d-1)$$

$$\mathrm{mindeg}_y T'_m \ge \min_{0 \le k \le m} \left(\left\lceil \tfrac{\mathrm{mindeg}_y T_k + (k+1)}{p} \right\rceil \right) - (m+1).$$

Proof. We prove the first inequality; the others follow similarly, the only difference being that r is replaced by 0. Define Laurent polynomials $U_{k,m}$ as in the proof of

Theorem 14, so that Equation (7) is satisfied modulo p^{j+1}, namely

$$\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+j+1} \equiv \sum_{m=0}^{j} U_{k,m} Q^{j-m} p^m \mod p^{j+1}. \tag{12}$$

We claim that

$$\deg_x U_{k,j} \leq \left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor + (k+j+1)h. \tag{13}$$

for all $j \in \{0, 1, \ldots, \alpha - k - 1\}$. By Lemma 15 (or indeed just by Proposition 5), the Laurent polynomial $U_{k,0}$ satisfies

$$\deg_x U_{k,0} \leq \left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor + (k+1)h.$$

Inductively, assume the claim is true for $U_{k,0}, \ldots, U_{k,j-1}$. For each $m \in \{0, 1, \ldots, j-1\}$, this implies

$$\deg_x(U_{k,m} Q^{j-m}) \leq \left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor + (k+j+1)h,$$

which is independent of m. By Lemma 15 with $\beta = j+1$, we have

$$\deg_x(\Lambda_{r,0}\big(T_k Q^{-k-1}\big)\, Q^{k+j+1}) \leq \left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor + (k+j+1)h.$$

The claim follows by combining the previous two sets of inequalities using Equation (12). Finally, for each m, by Lemma 9, Lemma 15, and the conditions on T_k, we have that each nonzero monomial $c\, x^I y^J$ in $U_{k,m}$ satisfies $J \geq -I$.

It remains to transfer the bounds on the Laurent polynomials $U_{k,j}$ to the digits $T'_m = \sum_{k=0}^{m} U_{k,m-k}$. Since the condition (13) holds for each $k \in \{0, 1, \ldots, \alpha - 1\}$, we have

$$\deg_x T'_m \leq \max_{0 \leq k \leq m} \left(\left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor + (m+1)h \right).$$

Also, for each m, by Lemma 9, each nonzero monomial $c\, x^I y^J$ in T'_m satisfies $J \geq -I$.

The carried digit from T'_m, when multiplied by Q, has x-degree at most $\deg_x T'_m + h$; this is already the x-degree bound on T'_{m+1}. Therefore the digits of the state $\lambda_{r,0}(S)$ satisfy the desired degree bounds. □

Corollary 21. *For each $r \in \{0, 1, \ldots, p-1\}$, we have $\lambda_{r,0}(\mathrm{val}_{p/Q}(\mathcal{W})) \subseteq \mathrm{val}_{p/Q}(\mathcal{W})$ and $\lambda_{r,0}(\mathrm{val}_{p/Q}(\mathcal{V})) \subseteq \mathrm{val}_{p/Q}(\mathcal{V})$. Furthermore if $r \neq 0$ then $\lambda_{r,0}(\mathrm{val}_{p/Q}(\mathcal{V})) \subseteq \mathrm{val}_{p/Q}(\mathcal{W})$.*

Proof. First let $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ such that $(T_{\alpha-1}, \ldots, T_1, T_0) := \mathrm{rep}_{p/Q}(S) \in \mathcal{W}$. By assumption, we have

$$\begin{aligned} \deg_x T_k &\leq (k+1)h - 1 \\ \deg_y T_k &\leq (k+1)(d-1) \\ \mathrm{mindeg}_y T_k &\geq -k. \end{aligned}$$

Proposition 20 now implies that $\lambda_{r,0}(S) \in \mathcal{W}$. The proof that $\mathrm{val}_{p/Q}(\mathcal{V})$ is closed under $\lambda_{r,0}$ is similar.

If $r \neq 0$, $\operatorname{rep}_{p/Q}(S) \in \mathcal{V}$, and $(T'_{\alpha-1}, \ldots, T'_1, T'_0) := \operatorname{rep}_{p/Q}(\lambda_{r,0}(S))$, then Proposition 20 tells us that

$$\begin{aligned}\deg_x T'_m &\leq \max_{0\leq k\leq m} \left(\left\lfloor \tfrac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor \right) + (m+1)h \\ &\leq \max_{0\leq k\leq m} \left(\left\lfloor \tfrac{-r}{p} \right\rfloor \right) + (m+1)h = (m+1)h - 1,\end{aligned}$$

Therefore $\operatorname{rep}_{p/Q}(\lambda_{r,0}(S)) \in \mathcal{W}$. □

Proposition 23 below tells us that the representations of most states belong to $\mathcal{W}$. For this we need the following lemma. Define $h_k = \deg_x(P \bmod p^{k+1})$ and $d_k = \deg_y(P \bmod p^{k+1})$; we have $h_0 = h$ and $d_0 = d$.

Lemma 22. *The base-$\frac{p}{Q}$ digits T_k of the initial state S_0 satisfy*

$$\begin{aligned}\deg_x T_k &\leq (k+1)h_k \\ \deg_y T_k &\leq (k+1)(d_k - 1) + 1 \\ \operatorname{mindeg}_y T_k &\geq -k,\end{aligned}$$

and every nonzero monomial $c\,x^I y^J$ that appears in T_k satisfies $J \geq -I$.

Proof. Recall that $S_0 = \left(y\frac{\partial P}{\partial y}\,(P/y)^{p^{\alpha-1}-1} \bmod p^\alpha \right)$. Define the digits T_k as in the proof of Theorem 17, namely

$$T_k = \left(\left(y\tfrac{\partial P}{\partial y} \cdot \tfrac{Q}{P/y} - T_0 - T_1\,(\tfrac{p}{Q}) - \cdots - T_{k-1}\,(\tfrac{p}{Q})^{k-1} \right) \left(\tfrac{Q}{p}\right)^k \bmod p \right).$$

First we consider the x-degree. For $T_0 = \left(y\frac{\partial P}{\partial y} \bmod p \right)$, we have $\deg_x T_0 \leq h_0$. For T_1, we use Lemma 18 to obtain $\deg_x \left(\frac{Q^2}{P/y} \bmod p^2 \right) \leq h_1$, which gives

$$\deg_x T_1 \leq \max(h_1 + h_1, h_0 + h_1) = 2h_1.$$

Inductively, for $k \geq 1$ we have

$$\begin{aligned}\deg_x T_k &\leq \max(h_k + kh_k, h_0 + kh_k, 2h_1 + (k-1)h_k, \ldots, kh_{k-1} + h_k) \\ &= (k+1)h_k.\end{aligned}$$

We now consider the y-degree. For T_0, we have $\deg_y T_0 \leq d_0$. For T_1, we use Lemma 18 to obtain $\deg_y \left(\frac{Q^2}{P/y} \bmod p^2 \right) \leq d_1 - 1$, which gives

$$\deg_y T_1 \leq \max(d_1 + d_1 - 1, d_0 + d_1 - 1) = 2d_1 - 1.$$

Inductively, for $k \geq 1$ we have

$$\begin{aligned}\deg_y T_k &\leq \max(d_k + k(d_k - 1), d_0 + k(d_k - 1), \ldots, k(d_{k-1} - 1) + 1 + d_k - 1) \\ &= (k+1)(d_k - 1) + 1.\end{aligned}$$

Finally, we consider the y-min-degree. We have $\operatorname{mindeg}_y T_0 \geq 0$. Inductively, $\operatorname{mindeg}_y T_k \geq -k$ by Lemma 18.

Lemma 9 gives the final condition. □

Proposition 23. *Let S_0 be the initial state, and let $(T_{\alpha-1}, \ldots, T_1, T_0) := \operatorname{rep}_{p/Q}(S_0)$. Let*

$$u = \left\lfloor \log_p \max(\alpha(h_{\alpha-1} - h), \alpha(d_{\alpha-1} - d) + 1) \right\rfloor + 1.$$

Then, for all $r_1, r_2, \ldots, r_u \in \{0, 1, \ldots, p-1\}$, *we have* $\mathrm{rep}_{p/Q}((\lambda_{r_u,0} \circ \cdots \circ \lambda_{r_2,0} \circ \lambda_{r_1,0})(S_0)) \in \mathcal{V}$.

Proof. Let S denote a state, $(T_{\alpha-1}, \ldots, T_1, T_0) = \mathrm{rep}_{p/Q}(S)$, $r \in \{0, \ldots, p-1\}$, and $(T'_{\alpha-1}, \ldots, T'_1, T'_0) = \mathrm{rep}_{p/Q}(\lambda_{r,0}(S))$. First we consider the y-min-degrees of states. By Proposition 20, if $\mathrm{mindeg}_y T_k \geq -k$ for $k \in \{0, 1, \ldots, \alpha-1\}$, then $\mathrm{mindeg}_y T'_m \geq -m$ for $m \in \{0, 1, \ldots, \alpha-1\}$. From Lemma 22, the digits of the initial state satisfy these constraints. Hence all states satisfy these constraints.

Next we consider the x-degree and y-degree of states. Assume that there is an $n \geq 0$ such that, for each $k \in \{0, 1, \ldots, \alpha-1\}$, the kth digit T_k of S satisfies

$$\begin{aligned} \deg_x T_k &\leq \left\lfloor \frac{(k+1)h_k - (k+1)h}{p^n} \right\rfloor + (k+1)h \\ \deg_y T_k &\leq \left\lfloor \frac{(k+1)d_k + 1 - (k+1)d}{p^n} \right\rfloor + (k+1)(d-1). \end{aligned} \tag{14}$$

Let $m \in \{0, 1, \ldots, \alpha-1\}$. Proposition 20 gives

$$\begin{aligned} \deg_x T'_m &\leq \max_{0 \leq k \leq m} \left(\left\lfloor \frac{\deg_x T_k - (k+1)h - r}{p} \right\rfloor \right) + (m+1)h \\ &\leq \max_{0 \leq k \leq m} \left(\left\lfloor \frac{\left\lfloor \frac{(k+1)h_k - (k+1)h}{p^n} \right\rfloor + (k+1)h - (k+1)h}{p} \right\rfloor \right) + (m+1)h \\ &\leq \max_{0 \leq k \leq m} \left(\left\lfloor \frac{(k+1)h_k - (k+1)h}{p^{n+1}} \right\rfloor \right) + (m+1)h. \end{aligned}$$

Since $h_k \leq h_m$ for each $k \in \{0, 1, \ldots, m\}$, this implies

$$\deg_x T'_m \leq \left\lfloor \frac{(m+1)h_m - (m+1)h}{p^{n+1}} \right\rfloor + (m+1)h.$$

Similarly,

$$\deg_y T'_m \leq \left\lfloor \frac{(m+1)d_m + 1 - (m+1)d}{p^{n+1}} \right\rfloor + (m+1)(d-1).$$

It follows that, if $\left\lfloor \frac{(m+1)h_m - (m+1)h}{p^{n+1}} \right\rfloor = 0$ and $\left\lfloor \frac{(m+1)d_m + 1 - (m+1)d}{p^{n+1}} \right\rfloor = 0$ for each m, then $\mathrm{rep}_{p/Q}(\lambda_{r,0}(S)) \in \mathcal{V}$.

We have shown that iterating $\lambda_{r,0}$ reduces the floor expression in (14). The initial state S_0 satisfies (14) with $n = 0$ since, by Lemma 22, the digits T_k of S_0 satisfy

$$\begin{aligned} \deg_x T_k &\leq (k+1)h_k \\ \deg_y T_k &\leq (k+1)(d_k - 1) + 1. \end{aligned}$$

It follows from the definition of u and the fact that $h_m \leq h_{\alpha-1}$ and $d_m \leq d_{\alpha-1}$ that $\left\lfloor \frac{(m+1)h_m - (m+1)h}{p^u} \right\rfloor = 0$ and $\left\lfloor \frac{(m+1)d_m + 1 - (m+1)d}{p^u} \right\rfloor = 0$ for each $m \in \{0, 1, \ldots, \alpha-1\}$. Therefore, for all $r_1, r_2, \ldots, r_u \in \{0, 1, \ldots, p-1\}$, we have $\mathrm{rep}_{p/Q}((\lambda_{r_u,0} \circ \cdots \circ \lambda_{r_2,0} \circ \lambda_{r_1,0})(S_0)) \in \mathcal{V}$. □

An immediate corollary of Proposition 23 is the following, where $|\mathcal{V}| = p^{\dim \mathcal{V}}$, since each coefficient in the digit T_k belongs to $D = \{0, 1, \ldots, p-1\}$, and where $\dim \mathcal{V}$ is given by Equation (11).

Corollary 24. *Let p be a prime, and let $\alpha \geq 1$. Let $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!]$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$ such that $h := \deg_x(P \bmod p) \geq 1$ and $d := \deg_y(P \bmod p) \geq 1$. Let*

$$u = \left\lfloor \log_p \max\big(\alpha(\deg_x(P \bmod p^\alpha) - h), \alpha(\deg_y(P \bmod p^\alpha) - d) + 1\big)\right\rfloor + 1. \quad (15)$$

Then

$$|\ker_p((a(n) \bmod p^\alpha)_{n\geq 0})| \leq p^{\frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha+(h+3)d+1)} + \tfrac{p^u-1}{p-1}.$$

In particular, for $\alpha = 1$ we have $|\ker_p((a(n) \bmod p)_{n\geq 0})| \leq p^{(h+1)d} + 1$. This is because Corollary 24 is also true with the u defined as in Proposition 23, and for $\alpha = 1$ we have $u = 1$ for this value.

By beginning to consider the orbit under $\lambda_{0,0}$, we obtain the following refinement of Corollary 24. For a function $f\colon X \to X$, define the *orbit* of $S \in X$ under f to be the sequence $S, f(S), f^2(S), \ldots$, and let $|\mathrm{orb}_f(S)|$ be the number of distinct terms in the orbit.

Corollary 25. *Let p be a prime, and let $\alpha \geq 1$. Let $F = \sum_{n\geq 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!]$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$ such that $h := \deg_x(P \bmod p) \geq 1$ and $d := \deg_y(P \bmod p) \geq 1$. Define u as in Equation (15). Then*

$$|\ker_p((a(n) \bmod p^\alpha)_{n\geq 0})| \leq p^{\frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha+hd+1)} + |\mathrm{orb}_{\Lambda_0}(F \bmod p^\alpha)| + \tfrac{p^u-1}{p-1} - u.$$

Proof. By Proposition 23, there are at most $\frac{p^u-1}{p-1}$ states that are not in $\mathcal{V}$. By Corollary 21, if $r \neq 0$ then $\lambda_{r,0}(\mathrm{val}_{p/Q}(\mathcal{V})) \subseteq \mathrm{val}_{p/Q}(\mathcal{W})$, and this is where the first term comes from, since the dimension of $\mathcal{W}$ is given by Equation (10). Applying $\lambda_{0,0}$ iteratively to S_0 produces $|\mathrm{orb}_{\lambda_{0,0}}(S_0)|$ states, and $|\mathrm{orb}_{\lambda_{0,0}}(S_0)| = |\mathrm{orb}_{\Lambda_0}(F \bmod p^\alpha)|$ by definition. The first u elements of $\mathrm{orb}_{\Lambda_0}(F \bmod p^\alpha)$ are already counted in the term $\frac{p^u-1}{p-1}$. The result follows. □

The structure of states given by Theorem 17 also provides a faster algorithm for computing the automaton by representing states as α-tuples of base-$\frac{p}{Q}$ digits rather than as Laurent polynomials. To make it efficient, we use tricks analogous to those we used for polynomial states [17]. The algorithm is as follows. First, for each $k \in \{0, 1, \ldots, \alpha-1\}$ and each $j \in \{0, 1, \ldots, \alpha-k-1\}$, compute the Laurent polynomial

$$Z_{j,k} := \left(\sum_{m=k+1}^{k+j+1} \binom{k+j+1}{m} Q^{pm-k-1} \Delta^{k+j+1-m} \bmod p^{j+1} \right)$$

from Equation (6) in the proof of Lemma 15 (where $\beta = j+1$), since these Laurent polynomials are used repeatedly and do not depend on the state S whose images $\lambda_{r,0}(S)$ we are computing at a given step. Then bin the monomials in each $Z_{j,k}$ according to their exponents modulo p. This allows us to compute, for each digit T_k that arises, the p images $\Lambda_{r,0}(T_k Z_{j,k})$ for $r \in \{0, 1, \ldots, p-1\}$ in one pass and without discarding any monomials.

5. Structure of the linear transformation $\lambda_{0,0}$

By Corollary 25, it remains to bound $|\mathrm{orb}_{\Lambda_0}(F)|$. In this section, we take the first step toward this goal by identifying univariate operators λ_0 that emulate $\lambda_{0,0}$ on three subspaces. The main result is Corollary 28.

Notation. Define the following coefficient-extraction maps. For a Laurent polynomial $S = \sum_{i,j} c_{i,j} x^i y^j$, define $\pi_{x,i}(S) = \sum_j c_{i,j} y^j$ and $\pi_{y,j}(S) = \sum_i c_{i,j} x^i$. The maps $\pi_{x,i}$ and $\pi_{y,j}$ allow us to focus on univariate (Laurent) polynomials by defining the following operator. Let $R \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$. Define $\lambda_0 \colon \mathcal{R}_{p^\alpha}[z, z^{-1}] \to \mathcal{R}_{p^\alpha}[z, z^{-1}]$ by

$$\lambda_0(S) = \Lambda_0\Big(SR^{p^\alpha - p^{\alpha-1}}\Big).$$

Let $\tilde{P} = yQ$. That is, $\tilde{P}$ is a lift of $P \bmod p$ which has the same monomial support as $P \bmod p$. Write

$$\tilde{P}(x, y) = \sum_{i \geq 0} x^i A_i(y) = \sum_{j \geq 0} B_j(x) y^j.$$

The univariate Laurent polynomials that will be used to define the various operators λ_0 are $R = \pi_{x,0}(Q) = A_0/y$, $R = \pi_{x,h}(Q) = A_h/y$, and $R = \pi_{y,d-1}(Q) = B_d$.

Proposition 26 below is analogous to [16, Proposition 13].

The following result is essentially a commutation relation. It shows that the left, right, and top borders of $\lambda_{0,0}(S)$ depend only on the respective borders of S, and therefore the behavior of $\lambda_{0,0}$ on these components is emulated by the respective operators λ_0. One checks that the conditions on S are satisfied by every state whose base-$\frac{p}{Q}$ representation belongs to $\mathcal{V}$, defined in Equation (9).

Proposition 26. *We have the following.*

(1) *Let $R = \pi_{x,0}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$,*

$$\pi_{x,0}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,0}(S)).$$

(2) *Let $R = \pi_{x,h}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ with height at most $p^{\alpha-1}h$,*

$$\pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,p^{\alpha-1}h}(S)).$$

(3) *Let $R = \pi_{y,d-1}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$ with degree at most $p^{\alpha-1}(d-1)$,*

$$\pi_{y,p^{\alpha-1}(d-1)}(\lambda_{0,0}(S)) = \lambda_0(\pi_{y,p^{\alpha-1}(d-1)}(S)).$$

Proof. We prove the second statement; the proofs of the others are analogous. Let $\pi_{\mathrm{r}} = \pi_{x,p^{\alpha-1}h}$, and let $\deg_x S \leq p^{\alpha-1}h$. Since π_{r} projects onto polynomials in y, we are interested in monomials with x-degree $p^{\alpha-1}h$ in $\lambda_{0,0}(S) = \Lambda_{0,0}\Big(SQ^{p^\alpha - p^{\alpha-1}}\Big)$. These come from monomials with x-degree $p^\alpha h$ in $SQ^{p^\alpha - p^{\alpha-1}}$. Since $\deg_x S \leq p^{\alpha-1}h$ and $\deg_x Q = h$, each monomial $c\, x^{p^\alpha h} y^J$ in $SQ^{p^\alpha - p^{\alpha-1}}$ arises only from the product of a monomial in $x^{p^{\alpha-1}h}\pi_{\mathrm{r}}(S)$ together with a product of $p^\alpha - p^{\alpha-1}$ monomials in $x^h \pi_{x,h}(Q)$, namely, monomials in $x^h A_h/y$. Therefore

$$\begin{aligned}
\pi_{\mathrm{r}}(\lambda_{0,0}(S)) &= \pi_{\mathrm{r}}(\lambda_{0,0}(x^{p^{\alpha-1}h}\pi_{\mathrm{r}}(S))) \\
&= \pi_{\mathrm{r}}\Big(\Lambda_{0,0}\Big(x^{p^{\alpha-1}h}\pi_{\mathrm{r}}(S) \cdot (x^h A_h/y)^{p^\alpha - p^{\alpha-1}}\Big)\Big) \\
&= \pi_{\mathrm{r}}\Big(x^{p^{\alpha-1}h}\Lambda_{0,0}\Big(\pi_{\mathrm{r}}(S)(A_h/y)^{p^\alpha - p^{\alpha-1}}\Big)\Big) \\
&= \Lambda_0\Big(\pi_{\mathrm{r}}(S)(A_h/y)^{p^\alpha - p^{\alpha-1}}\Big) \\
&= \lambda_0(\pi_{\mathrm{r}}(S)),
\end{aligned}$$

where in the third equality we use Proposition 5 to rewrite $\Lambda_{0,0}(Gx^{p^\alpha h}) = x^{p^{\alpha-1}h}\Lambda_{0,0}(G)$. □

We introduce the following projection maps on base-$\frac{p}{Q}$ representations.

Notation. For $z \in \{x, y\}$ and $i \geq 0$, define

$$\mathrm{pr}_{z,i}((T_{\alpha-1}, \ldots, T_0)) = (\pi_{z,\alpha i}(T_{\alpha-1}), \ldots, \pi_{z,i}(T_0)).$$

The next result tells us that the operation of converting to digit representations commutes with projecting onto one of the borders. We need the following notation.

Notation. Given a univariate Laurent polynomial $R \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$, we define $\mathrm{rep}_{p/R}$ analogously to $\mathrm{rep}_{p/Q}$ in Equation (5). Namely, $\mathrm{rep}_{p/R}\left(\sum_{k=0}^{\alpha-1} T_k\,(\frac{p}{R})^k R^{p^{\alpha-1}-1}\right) := (T_{\alpha-1}, \ldots, T_1, T_0)$.

Theorem 27. *Let S be a state in $\mathrm{val}_{p/Q}(\mathcal{V})$.*

1. *Let $R = \pi_{x,0}(Q)$. Then $\mathrm{pr}_{x,0}(\mathrm{rep}_{p/Q}(S)) = \mathrm{rep}_{p/R}(\pi_{x,0}(S))$.*
2. *Let $R = \pi_{x,h}(Q)$. Then $\mathrm{pr}_{x,h}(\mathrm{rep}_{p/Q}(S)) = \mathrm{rep}_{p/R}(\pi_{x,p^{\alpha-1}h}(S))$.*
3. *Let $R = \pi_{y,d-1}(Q)$. Then $\mathrm{pr}_{y,d-1}(\mathrm{rep}_{p/Q}(S)) = \mathrm{rep}_{p/R}(\pi_{y,p^{\alpha-1}(d-1)}(S))$.*

Proof. Let $(T_{\alpha-1}, \ldots, T_1, T_0) = \mathrm{rep}_{p/Q}(S)$, so that

$$S = \left(\sum_{k=0}^{\alpha-1} T_k\,(\tfrac{p}{Q})^k\right) Q^{p^{\alpha-1}-1}.$$

We prove the second statement; the others are analogous. We have

$$\pi_{x,p^{\alpha-1}h}(S) = \sum_{k=0}^{\alpha-1} \pi_{x,p^{\alpha-1}h}\left(T_k p^k Q^{p^{\alpha-1}-1-k}\right).$$

Since $\mathrm{rep}_{p/Q}(S) \in \mathcal{V}$, the digit T_k has x-degree at most $(k+1)h$. The only way to get a monomial in $T_k Q^{p^{\alpha-1}-1-k}$ with x-degree $p^{\alpha-1}h$ is to multiply a monomial in T_k with x-degree $(k+1)h$ by a monomial in $Q^{p^{\alpha-1}-1-k}$ with x-degree $(p^{\alpha-1}-1-k)h$. Therefore

$$\begin{aligned}
\pi_{x,p^{\alpha-1}h}(S) &= \sum_{k=0}^{\alpha-1} \pi_{x,(k+1)h}(T_k)\, p^k \pi_{x,(p^{\alpha-1}-1-k)h}\left(Q^{p^{\alpha-1}-1-k}\right) \\
&= \sum_{k=0}^{\alpha-1} \pi_{x,(k+1)h}(T_k)\, p^k (\pi_{x,h}(Q))^{p^{\alpha-1}-1-k} \\
&= \sum_{k=0}^{\alpha-1} \pi_{x,(k+1)h}(T_k)\, p^k R^{p^{\alpha-1}-1-k} \\
&= \left(\sum_{k=0}^{\alpha-1} \pi_{x,(k+1)h}(T_k)\,(\tfrac{p}{R})^k\right) R^{p^{\alpha-1}-1}.
\end{aligned}$$

This implies $\mathrm{rep}_{p/R}(\pi_{x,p^{\alpha-1}h}(S)) = \mathrm{pr}_{x,h}(\mathrm{rep}_{p/Q}(S))$, as claimed. □

Proposition 26 and Theorem 27, which are both commutation statements involving projection, culminate in the following.

Corollary 28. *Let S be a state in $\mathrm{val}_{p/Q}(\mathcal{V})$.*

(1) *Let* $R = \pi_{x,0}(Q)$. *Then* $\mathrm{pr}_{x,0}(\mathrm{rep}_{p/Q}(\lambda_{0,0}(S))) = \mathrm{rep}_{p/R}(\lambda_0(\pi_{x,0}(S)))$.
(2) *Let* $R = \pi_{x,h}(Q)$. *Then* $\mathrm{pr}_{x,h}(\mathrm{rep}_{p/Q}(\lambda_{0,0}(S))) = \mathrm{rep}_{p/R}(\lambda_0(\pi_{x,p^{\alpha-1}h}(S)))$.
(3) *Let* $R = \pi_{y,d-1}(Q)$. *Then* $\mathrm{pr}_{y,d-1}(\mathrm{rep}_{p/Q}(\lambda_{0,0}(S))) = \mathrm{rep}_{p/R}(\lambda_0(\pi_{y,p^{\alpha-1}(d-1)}(S)))$.

Proof. We prove the second statement; the other proofs are similar. Since $S \in \mathrm{val}_{p/Q}(\mathcal{V})$, then by Corollary 21, $\lambda_{0,0}(S) \in \mathrm{val}_{p/Q}(\mathcal{V})$. Therefore we can apply Theorem 27 to give $\mathrm{pr}_{x,h}(\mathrm{rep}_{p/Q}(\lambda_{0,0}(S))) = \mathrm{rep}_{p/R}(\pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)))$. Again because $S \in \mathrm{val}_{p/Q}(\mathcal{V})$, it satisfies the conditions of Proposition 26, so that $\pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,p^{\alpha-1}h}(S))$. Putting these two equations together, we get the second statement. □

6. Period lengths of series expansions modulo p and modulo p^α

In this section, we state theorems of Engstrom [9] that bound period lengths of coefficient sequences of rational series modulo p and modulo p^α. We then apply these theorems to bound the period length of the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ in Corollary 34.

The following is a strengthening of Engstrom [9, Theorems 2 and 3], who bounds the period length of the coefficient sequence of a rational series $\frac{1}{R}$. In Theorem 29 we reduce his bound by a factor of p when e is a power of p.

Theorem 29. *Let* $R \in \mathbb{F}_p[z]$ *be a polynomial with* $R(0) \neq 0$ *and* $\deg R \geq 1$. *Factor* $R = cR_1^{e_1} \cdots R_k^{e_k}$ *into monic irreducibles. Let* $e = \max_{1 \leq i \leq k} e_i$ *and* $L = \mathrm{lcm}_{1 \leq i \leq k}(p^{\deg R_i} - 1)$. *Then the coefficient sequence of* $\frac{1}{R}$ *is periodic with period length dividing* $p^{\lceil \log_p e \rceil} L$.

Proof. Lift R and $R_1, \ldots, R_k$ to $\mathbb{Z}_p[z]$, and write $\frac{1}{R} = \sum_{n \geq 0} a(n) z^n \in \mathbb{Z}_p[\![z]\!]$. We follow Engstrom [9, Section 3.1]. For $i \in \{1, 2, \ldots, k\}$ and $j \in \{1, 2, \ldots, \deg R_i\}$, let $\rho_{i,j}$ be the jth root of $R_i(z) = 0$. Then, for all $n \geq 0$, we have

$$a(n) = \sum_{i,j} \left(c_{i,j,0} \binom{n}{0} + c_{i,j,1} \binom{n}{1} + \cdots + c_{i,j,e_i-1} \binom{n}{e_i - 1} \right) \rho_{i,j}^n$$

for some elements $c_{i,j,j'}$ in the splitting field of R over $\mathbb{Q}_p$. Engstrom [9, Lemma 4] implies that each $c_{i,j,j'}$ is a p-adic algebraic integer. The appropriate generalization of Fermat's little theorem implies that $\rho_{i,j}^{p^{\deg R_i} - 1} \equiv 1 \mod p$. Therefore the period length of $(\rho_{i,j}^n \bmod p)_{n \geq 0}$ divides L. It remains to bound the period lengths modulo p of $\binom{n}{0}, \ldots, \binom{n}{e_i - 1}$. A result of Ząbek [22, Théorème 3] implies that the period length of $(\binom{n}{j'} \bmod p)_{n \geq 0}$ is $p^{\lfloor \log_p j' \rfloor + 1} \leq p^{\lfloor \log_p (e_i - 1) \rfloor + 1} \leq p^{\lfloor \log_p (e-1) \rfloor + 1} = p^{\lceil \log_p e \rceil}$. The result follows. □

Theorem 30 (Engstrom [9, Theorem 8])**.** *Let* $T \in \mathcal{R}_{p^\alpha}[z]$ *be a polynomial with* $t := \deg T \geq 1$ *such that the coefficients of* z^0 *and* z^t *in* T *are nonzero modulo* p. *Write* $\frac{1}{T} = \sum_{n \geq 0} a(n) z^n$, *and let* m *be the period length of* $(a(n) \bmod p)_{n \geq 0}$. *Then* $a(n)_{n \geq 0}$ *is periodic with period length dividing* $p^{\alpha-1} m$.

Example 31. Let $p = 2$, $\alpha = 2$, and $R = -z^2 - z + 1 \in \mathcal{R}_4[z]$. Let $T := R^{p^{\alpha-1}} = (-z^2 - z + 1)^2$. Since $R \bmod 2$ is irreducible, the quantities in Theorem 29 are $e = 2$ and $L = 2^2 - 1 = 3$. Theorem 29 implies that the coefficient sequence of $\frac{1}{T} \bmod p$ is periodic with period length m dividing $p^{\lceil \log_p e \rceil} L = 2^1 \cdot 3 = 6$, and in fact the period length is $m = 6$. Theorem 30 then implies that the coefficient sequence of $\frac{1}{T}$

is periodic with period length dividing $p^{\alpha-1}m = 12$, and in fact the period length is 12.

We will also use the following lemma, which is interesting in its own right. It establishes that the period of the coefficient sequence of the series $\frac{1}{T}$ ends with zeros. For example, consider $T = -z^2 - z + 1 \in \mathbb{Q}[z]$, whose coefficient sequence of $\frac{1}{T}$ is the shifted Fibonacci sequence $1, 1, 2, 3, 5, 8, \ldots$; the following lemma implies that its period modulo p ends with exactly 1 zero.

Lemma 32. *Let $T \in \mathcal{R}_{p^\alpha}[z]$ be a polynomial with $t := \deg T \geq 1$. If the coefficients of z^0 and z^t in T are nonzero modulo p, then the coefficient sequence of $\frac{1}{T}$ is periodic, and its period ends with exactly $t-1$ zeros.*

Proof. Write $T = \sum_{i=0}^{t} c_i z^i$ and $\frac{1}{T} = \sum_{n\geq 0} a(n) z^n$. The sequence $a(n)_{n\geq 0}$ is periodic by a standard argument using the invertibility of c_0 and $t \geq 1$. In what follows, we use periodicity to relate the end of the period to the beginning of the sequence. We iterate an argument which gives one zero at each step.

Comparing coefficients on both sides of the equation $T \sum_{n\geq 0} a(n) z^n = 1$, we obtain $c_0 a(0) = 1$ and

$$c_{t-i}a(0) + c_{t-i-1}a(1) + \cdots + c_0 a(t-i) = 0 \tag{16}$$

for all i in the range $1 \leq i \leq t-1$. Moreover, for all $n \geq 0$ we have the recurrence

$$c_t a(n) + c_{t-1}a(n+1) + c_{t-2}a(n+2) + \cdots + c_0 a(n+t) = 0. \tag{17}$$

Let m be the period length of $a(n)_{n\geq 0}$.

As $m \geq 1$, we can set $n = m-1$ in Equation (17). The periodicity of $a(n)_{n\geq 0}$ and Equation (16) with $i = 1$ gives

$$\begin{aligned} c_t a(m-1) &= -c_{t-1}a(m) - c_{t-2}a(m+1) - \cdots - c_0 a(m-1+t) \\ &= -c_{t-1}a(0) - c_{t-2}a(1) - \cdots - c_0 a(t-1) \\ &= 0. \end{aligned}$$

Since c_t is invertible, we have $a(m-1) = 0$. As $a(0) \neq 0$, this implies $m \geq 2$.

Therefore, we can set $n = m-2$ in Equation (17). Periodicity, $a(m-1) = 0$, and Equation (16) with $i = 2$ gives

$$\begin{aligned} c_t a(m-2) &= -c_{t-1}a(m-1) - c_{t-2}a(m) - \cdots - c_0 a(m-2+t) \\ &= 0 - c_{t-2}a(0) - \cdots - c_0 a(t-2) \\ &= 0. \end{aligned}$$

Iterating this argument for $i \in \{3, 4, \ldots, t-2\}$, we obtain $a(n) = 0$ for all n satisfying $m - (t-2) \leq n \leq m-1$ and $m \geq t-1$.

Setting $n = m - (t-1)$ and $i = t-1$ gives

$$\begin{aligned} c_t a(m-t+1) &= -c_{t-1}a(m-t+2) - \cdots - c_2 a(m-1) - c_1 a(m) - c_0 a(m+1) \\ &= 0 + \cdots + 0 - c_1 a(0) - c_0 a(1) \\ &= 0. \end{aligned}$$

Therefore $a(n) = 0$ for all n satisfying $m - (t-1) \leq n \leq m-1$ and $m \geq t$.

Finally, setting $n = m - t$ gives

$$\begin{aligned} c_t a(m-t) &= -c_{t-1}a(m-t+1) - \cdots - c_1 a(m-1) - c_0 a(m) \\ &= 0 + \cdots + 0 - c_0 a(0) \\ &= -1, \end{aligned}$$

leaving exactly $t-1$ zeros at the end of the period of $a(n)_{n\geq 0}$. □

The following corollary of Lemma 32 tells us that certain Laurent polynomials produce periodic series expansions.

Corollary 33. *Let $T \in \mathcal{R}_{p^\alpha}[z]$ such that $t := \deg T \geq 1$ and the coefficients of z^0 and z^t in T are nonzero modulo p. For all i in the range $0 \leq i \leq t-1$, the coefficient sequence of $\frac{1}{z^{-i}T}$ is periodic, and its period begins with i zeros and ends with $t-1-i$ zeros.*

We next combine Corollary 33 with Engstrom's bounds to get information on the period lengths of the coefficient sequences of $\frac{1}{R \bmod p}$ and $\frac{1}{R^{p^{\alpha-1}}}$ in the case that $R \in z^{-1}\mathcal{R}_{p^\alpha}[z]$. These period lengths depend on $R \bmod p$. Its *factorization into irreducibles* is $(R \bmod p) = cz^{e_0}R_1^{e_1}\cdots R_k^{e_k}$, where $z, R_1, \ldots, R_k \in \mathbb{F}_p[z]$ are distinct, monic, irreducible polynomials, $c \in \mathbb{F}_p$, $e_0 \geq -1$, and $e_i \geq 1$ for all $i \in \{1, \ldots, k\}$. If $(R \bmod p) \neq 0$, define $\deg(R \bmod p)$ to be the largest exponent of z with a nonzero coefficient in the expansion of $R \bmod p$ in the monomial basis. Finally, let $\nu_p(m)$ denote the p-adic valuation of m.

Corollary 34. *Let $R \in z^{-1}\mathcal{R}_{p^\alpha}[z]$ be a nonzero Laurent polynomial. Factor $(R \bmod p) = cz^{e_0}R_1^{e_1}\cdots R_k^{e_k}$ into irreducibles. Suppose that $e_0 \in \{-1, 0\}$ and $\deg(R \bmod p) \geq 1$. Then the coefficient sequence of $\frac{1}{R \bmod p}$ is periodic, and its period length m satisfies $\nu_p(m) \leq \lceil \log_p \max(e_1, \ldots, e_k) \rceil$. Moreover, the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ is periodic, and its period length divides $p^{2(\alpha-1)}m$.*

Proof. First we address the series $\frac{1}{R \bmod p}$. If $e_0 = 0$, then Theorem 29 already tells us that its coefficient sequence is periodic and that its period length m satisfies $\nu_p(m) \leq \lceil \log_p \max(e_1, \ldots, e_k) \rceil$. If $e_0 = -1$, we write $\frac{1}{R \bmod p} = \frac{1}{z^{-1}(zR \bmod p)}$ and apply Corollary 33 to conclude that the coefficient sequence of $\frac{1}{R \bmod p}$ is periodic with the same period length as $\frac{1}{zR \bmod p}$; since zR is a polynomial, the period length m satisfies $\nu_p(m) \leq \lceil \log_p \max(e_1, \ldots, e_k) \rceil$ by Theorem 29.

Next we show that the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ is periodic. Since the coefficient of z^{e_0} is nonzero in $R \bmod p$ and $e_0 \leq 0$, we have a power series expansion for $\frac{1}{R^{p^{\alpha-1}}}$. Let $r := \deg(R \bmod p)$.

If $e_0 = 0$, we apply Lemma 6 to see that $\frac{1}{R^{p^{\alpha-1}}} \equiv \frac{1}{(R \bmod p)^{p^{\alpha-1}}} \mod p^\alpha$. Since the leading coefficient of $R \bmod p$ is nonzero modulo p, the leading coefficient of $(R \bmod p)^{p^{\alpha-1}}$ is nonzero modulo p^α. Then, since $r \geq 1$, the coefficient sequence of $\frac{1}{(R \bmod p)^{p^{\alpha-1}}}$ is periodic. This implies that the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ is periodic.

If $e_0 = -1$, (using Lemma 6 again) we apply Lemma 32 to $T := (zR)^{p^{\alpha-1}} = (zR \bmod p)^{p^{\alpha-1}}$, whose degree is $p^{\alpha-1}(r+1)$. Since $r \geq 1$, we deduce that the period of the coefficient sequence of $\frac{1}{T}$ ends with $p^{\alpha-1}(r+1) - 1 \geq p^{\alpha-1}$ zeros. As

$R^{p^{\alpha-1}} = z^{-p^{\alpha-1}}T$, we can apply Corollary 33 with $i = p^{\alpha-1}$ to conclude that the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ is periodic.

Finally we bound the period length of $\frac{1}{R^{p^{\alpha-1}}}$. To do this, we first bound the period length of $\frac{1}{R^{p^{\alpha-1}}} \bmod p$. Since $\mathbb{F}_p$ has characteristic p, we have $\frac{1}{R(z)^p} \equiv \frac{1}{R(z^p)} \bmod p$, so that raising $\frac{1}{R}$ to the power p causes its coefficient sequence modulo p to dilate by a factor of p. Iterating, we get $\frac{1}{R(z)^{p^{\alpha-1}}} \equiv \frac{1}{R(z^{p^{\alpha-1}})} \bmod p$. Therefore the period length of $\frac{1}{R^{p^{\alpha-1}}} \bmod p$ divides $p^{\alpha-1}m$.

Now we use the period length of $\frac{1}{R^{p^{\alpha-1}}} \bmod p$ to bound the period length of $\frac{1}{R^{p^{\alpha-1}}}$ modulo p^α. We apply Theorem 30 with $T = R^{p^{\alpha-1}}$ to see that the period length of the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ divides $p^{2(\alpha-1)}m$. □

7. Orbit size of a univariate Laurent polynomial under λ_0

In this section, our goal is to prove Corollary 43, which tells us that the orbit of a univariate Cartier operator λ_0 is finite, and which gives bounds on the transient and period length of this orbit.

We begin with the following result, which lets us restrict attention to Laurent polynomials S with $\deg S \le p^{\alpha-1}\deg(R \bmod p)$ in Theorems 38, 40, and 41. The proof uses the fact that if $f(x) = \left\lfloor \frac{x-p^{\alpha-1}r}{p} \right\rfloor + p^{\alpha-1}r$, then, for every $x \ge p^{\alpha-1}r$ and $n \ge \lfloor \log_p(x - p^{\alpha-1}r) \rfloor + 1$, we have $f^n(x) = p^{\alpha-1}r$.

Lemma 35. *Let $R \in z^{-1}\mathcal{R}_{p^\alpha}[z]$ be a Laurent polynomial, let $r = \deg(R \bmod p)$, and define λ_0 on $\mathcal{R}_{p^\alpha}[z, z^{-1}]$ by $\lambda_0(S) = \Lambda_0\left(SR^{p^\alpha - p^{\alpha-1}}\right)$. Let $S \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$, let $s = \deg S$, and suppose that $s > p^{\alpha-1}r$. If $n \ge \lfloor \log_p(s - p^{\alpha-1}r) \rfloor + 1$, then $\deg \lambda_0^n(S) \le p^{\alpha-1}r$.*

Our strategy is to transfer periodicity of a series expansion to eventual periodicity of the orbit under λ_0. We first illustrate with an example.

Example 36. As in Example 31, let $p = 2$, $\alpha = 2$, and $R = -z^2 - z + 1 \in \mathcal{R}_4[z]$. Write $\frac{1}{R^{p^{\alpha-1}}} = \frac{1}{R^2} = \sum_{n\ge 0} a(n)z^n \in \mathcal{R}_4[\![z]\!]$. The sequence $a(n)_{n\ge 0}$ is periodic with period length 12. In light of Lemma 35, we consider Laurent polynomials $S \in \mathcal{R}_4[z]$ such that $-1 = 1 - p^{\alpha-1} \le \operatorname{mindeg} S$ and $\deg S \le p^{\alpha-1}\deg(R \bmod p) = 4$. Let $j \in \{-1, 0, 1, 2, 3, 4\}$, so that each monomial in S is of the form $c\,z^j$. By Proposition 5,

$$\lambda_0(z^j) = \Lambda_0(z^j R^2) = \Lambda_0(\tfrac{z^j}{R^2} R^4) = \Lambda_0(\tfrac{z^j}{R^2})R^2.$$

If $j = -1$, it can be verified that $\lambda_0(z^{-1}) = 0$. For $j \in \{0, 1, 2, 3, 4\}$, we show that $\Lambda_0^4(\frac{z^j}{R^2}) = \Lambda_0^2(\frac{z^j}{R^2})$, so that

$$\lambda_0^4(z^j) = \Lambda_0^4(\tfrac{z^j}{R^2})R^2 = \Lambda_0^2(\tfrac{z^j}{R^2})R^2 = \lambda_0^2(z^j).$$

Since $\frac{z^j}{R^2} = \sum_{n\ge j} a(n-j)z^n$ and $\Lambda_0^2(z^n) = 0$ if $n \not\equiv 0 \bmod 4$, we have

$$\Lambda_0^2\left(\frac{z^j}{R^2}\right) = \Lambda_0^2\left(\sum_{n \ge \lceil j/4 \rceil} a(4n-j)z^{4n}\right) = \sum_{n \ge \lceil j/4 \rceil} a(4n-j)z^n.$$

Similarly,

$$\Lambda_0^4\left(\frac{z^j}{R^2}\right) = \Lambda_0^2\left(\sum_{n\geq\lceil j/4\rceil} a(4n-j)z^n\right) = \sum_{n\geq\lceil j/16\rceil} a(16n-j)z^n.$$

Since $4n-j \equiv 16n-j \mod 12$ and $\lceil j/4\rceil = \lceil j/16\rceil$ for $j\in\{0,1,2,3,4\}$, it follows that $\Lambda_0^4(\frac{z^j}{R^2}) = \Lambda_0^2(\frac{z^j}{R^2})$, as desired. By linearity, this implies $\lambda_0^4(S) = \lambda_0^2(S)$ for all $S\in\mathcal{R}_4[z]$ with $-1\leq \operatorname{mindeg} S$ and $\deg S\leq 4$.

Let $\operatorname{ord}_m(p)$ be the eventual period length of the sequence $(p^n \bmod m)_{n\geq 0}$. That is, $\operatorname{ord}_m(p)$ is the smallest integer $k\geq 1$ such that $p^{n+k}\equiv p^n \mod m$ for all sufficiently large n. When p and m are relatively prime, $\operatorname{ord}_m(p)$ is the usual multiplicative order of p modulo m. When p and m are not relatively prime, then $\operatorname{ord}_m(p) = \operatorname{ord}_{m'}(p)$ where $m = p^{\nu_p(m)}m'$.

Engstrom's Theorems 29 and 30 let us bound the eventual period length m of $\frac{1}{R \bmod p}$, and in Corollary 34 we showed that the period length of the expansion of $\frac{1}{R^{p^{\alpha-1}}}$ divides $p^{2(\alpha-1)}m$. We will see that the orbit size under λ_0 is related to m. Since $\Lambda_0^k\left(\sum_{n\geq 0} a(n)z^n\right) = \sum_{n\geq 0} a(p^k n)z^n$, if $a(n)_{n\geq 0}$ has period length m then $\operatorname{ord}_m(p)$ determines the generic orbit size under Λ_0. We will use the next lemma to evaluate it.

Lemma 37. *Let $p\geq 2$ be an integer, let $r_1,\ldots,r_k$ be positive integers, and let $L = \operatorname{lcm}_{1\leq i\leq k}(p^{r_i}-1)$. Then $\operatorname{ord}_L(p) = \operatorname{lcm}(r_1,\ldots,r_k)$.*

Proof. For each i, we have that $p^{r_i}-1$ divides $p^{\operatorname{lcm}(r_1,\ldots,r_k)}-1$. Therefore L divides $p^{\operatorname{lcm}(r_1,\ldots,r_k)}-1$. It follows that $p^{\operatorname{lcm}(r_1,\ldots,r_k)}-1\equiv 0 \mod L$, and therefore $\operatorname{ord}_L(p)$ divides $\operatorname{lcm}(r_1,\ldots,r_k)$.

It remains to show that $\operatorname{lcm}(r_1,\ldots,r_k)$ divides $\operatorname{ord}_L(p)$. For each i, the definition of $\operatorname{ord}_{p^{r_i}-1}(p)$ implies $p^{\operatorname{ord}_{(p^{r_i}-1)}(p)}\equiv 1 \mod p^{r_i}-1$. It follows that $p^{r_i}-1$ divides $p^{\operatorname{ord}_{(p^{r_i}-1)}(p)}-1$. Since $p^a-1 \mid p^b-1$ implies $a\mid b$, we have $r_i \mid \operatorname{ord}_{p^{r_i}-1}(p)$. By the definition of L, we have $p^{r_i}-1\mid L$, so this implies $r_i\mid \operatorname{ord}_L(p)$. Every prime power dividing $\operatorname{lcm}(r_1,\ldots,r_k)$ divides some r_i, so $\operatorname{lcm}(r_1,\ldots,r_k)$ divides $\operatorname{ord}_L(p)$. □

The next several results establish the orbit size under λ_0 in various settings. We start with Theorem 38, where we assume that $\deg(R \bmod p)\geq 1$ and $\operatorname{mindeg}(R \bmod p)\in\{-1,0\}$. Then we consider $\operatorname{mindeg}(R \bmod p)\geq 1$ in Theorem 40. Finally in Theorems 41 and 42, we deal with the remaining possibilities. The statement of Corollary 43 covers all cases.

Theorem 38. *Let $R\in z^{-1}\mathcal{R}_{p^\alpha}[z]$ be a nonzero Laurent polynomial. Factor $(R \bmod p) = cz^{e_0}R_1^{e_1}\cdots R_k^{e_k}$ into irreducibles. Suppose that $e_0\in\{-1,0\}$ and $\deg(R \bmod p)\geq 1$. Let $\ell = \operatorname{lcm}(\deg R_1,\ldots,\deg R_k)$. Define λ_0 on $\mathcal{R}_{p^\alpha}[z,z^{-1}]$ by $\lambda_0(S) = \Lambda_0\left(SR^{p^\alpha-p^{\alpha-1}}\right)$. If $S\in\mathcal{R}_{p^\alpha}[z,z^{-1}]$ with $1-p^{\alpha-1}\leq \operatorname{mindeg} S$ and $\deg S\leq p^{\alpha-1}\deg(R \bmod p)$, then*

$$\lambda_0^{n+\ell}(S) = \lambda_0^n(S)$$

for all $n\geq \lceil \log_p \max(e_1,\ldots,e_k)\rceil + 2(\alpha-1)$.

In particular, the eventual period length of the orbit is independent of α.

Proof. Let $r := \deg(R \bmod p)$. By Corollary 34, the coefficient sequence of $\frac{1}{R \bmod p}$ is periodic, and its period length m satisfies $\nu_p(m) \le \lceil \log_p \max(e_1, \ldots, e_k) \rceil$. Let $t := \nu_p(m) + 2(\alpha - 1)$. We will show that if $n \ge t$, then $\lambda_0^{n+\mathrm{ord}_m(p)}(S) = \lambda_0^n(S)$. Then, by Theorem 29, m divides $p^{\lceil \log_p \max(e_1,\ldots,e_k) \rceil} L$, where $L = \mathrm{lcm}_{1 \le i \le k}(p^{\deg R_i} - 1)$. Since $\gcd(L, p) = 1$, we have $\mathrm{ord}_m(p) = \mathrm{ord}_L(p)$. Applying Lemma 37 with $r_i = \deg R_i$ gives that $\mathrm{ord}_m(p) = \ell$, and the theorem statement will follow.

Corollary 34 also tells us that the coefficient sequence of $\frac{1}{R^{p^{\alpha-1}}}$ is periodic with period length dividing $p^{2(\alpha-1)}m$. Therefore $\Lambda_0^t\left(\frac{1}{R^{p^{\alpha-1}}}\right)$ has period length dividing m. Write $\frac{1}{R^{p^{\alpha-1}}} = \sum_{n \ge 0} a(n) z^n \in \mathcal{R}_{p^\alpha}[\![z]\!]$. The period of $a(n)_{n \ge 0}$ ends with exactly $p^{\alpha-1}r - 1$ zeros; this follows from Corollary 33 when $e_0 = 0$ and is proved in the proof of Corollary 34 when $e_0 = -1$. In other words, we have

$$a(p^{2(\alpha-1)}m - i) = 0 \tag{18}$$

for all $i \in \{1, \ldots, p^{\alpha-1}r - 1\}$.

Let $j \in \{1 - p^{\alpha-1}, \ldots, p^{\alpha-1}r\}$. By Proposition 5,

$$\lambda_0(z^j) = \Lambda_0\left(z^j R^{p^\alpha - p^{\alpha-1}}\right) = \Lambda_0\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) R^{p^{\alpha-1}}. \tag{19}$$

Therefore, by iterating, $\lambda_0^n(z^j) = \Lambda_0^n\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) R^{p^{\alpha-1}}$ for all $n \ge 0$. We show

$$\Lambda_0^{t+\mathrm{ord}_m(p)}\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) = \Lambda_0^t\left(\frac{z^j}{R^{p^{\alpha-1}}}\right);$$

this implies $\lambda_0^{t+\mathrm{ord}_m(p)}(z^j) = \lambda_0^t(z^j)$, and the statement will follow from the linearity of λ_0. Since $\Lambda_0^k(z^n) = 0$ if $n \not\equiv 0 \mod p^k$, we have

$$\begin{aligned}\Lambda_0^t\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) &= \Lambda_0^t\left(\sum_{n \ge j} a(n-j) z^n\right) = \Lambda_0^t\left(\sum_{n \ge \lceil j/p^t \rceil} a(p^t n - j) z^{p^t n}\right) \\ &= \sum_{n \ge \lceil j/p^t \rceil} a(p^t n - j) z^n.\end{aligned}$$

Similarly,

$$\Lambda_0^{t+\mathrm{ord}_m(p)}\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) = \sum_{n \ge \lceil j/p^{t+\mathrm{ord}_m(p)} \rceil} a(p^{t+\mathrm{ord}_m(p)} n - j) z^n.$$

Recall that $a(n)_{n \ge 0}$ is periodic with period length dividing $p^{2(\alpha-1)}m$. Since $p^{t+\mathrm{ord}_m(p)} \equiv p^t \mod p^{2(\alpha-1)}m$, we have $a(p^{t+\mathrm{ord}_m(p)} n - j) = a(p^t n - j)$ for all n such that $p^t n - j \ge 0$, that is, when $n \ge \lceil j/p^t \rceil$. Therefore

$$\Lambda_0^{t+\mathrm{ord}_m(p)}\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) - \Lambda_0^t\left(\frac{z^j}{R^{p^{\alpha-1}}}\right) = \sum_{n = \lceil j/p^{t+\mathrm{ord}_m(p)} \rceil}^{\lceil j/p^t \rceil - 1} a(p^{t+\mathrm{ord}_m(p)} n - j) z^n. \tag{20}$$

If $j \le 1$, then this sum is empty and therefore 0. So assume $j \in \{2, \ldots, p^{\alpha-1}r\}$. It remains to show that $a(p^{t+\mathrm{ord}_m(p)} n - j) = 0$ for all n in the range of summation of the sum in Equation (20).

Take n in the range of summation $\{\lceil j/p^{t+\mathrm{ord}_m(p)} \rceil, \ldots, \lceil j/p^t \rceil - 1\}$ in Equation (20). We have $j - n \in \{j + 1 - \lceil j/p^t \rceil, \ldots, j - \lceil j/p^{t+\mathrm{ord}_m(p)} \rceil\}$. Since $2 \le j \le$

$p^{\alpha-1}r$, it follows with generosity that $j-n \in \{1,\dots,p^{\alpha-1}r-1\}$. The period length of $a(n)_{n\geq 0}$ divides $p^{2(\alpha-1)}m$, so $a(p^{2(\alpha-1)}mn+n-j) = a(p^{2(\alpha-1)}m-(j-n))$. Since $a(p^{2(\alpha-1)}m-(j-n)) = 0$ by Equation (18), this implies $a(p^{2(\alpha-1)}mn+n-j) = 0$, as desired. □

Next we show that, if R is a polynomial and is divisible by z, then elements sufficiently far out in orbits under λ_0 are also divisible by a certain power of z.

Proposition 39. *Let $R \in \mathcal{R}_{p^\alpha}[z]$ be a nonzero polynomial such that $(R \bmod p) = z^{e_0}G$ for some $G \in \mathbb{F}_p[z]$ where $e_0 \geq 1$ and G is not divisible by z. If $S \in \mathcal{R}_{p^\alpha}[z,z^{-1}]$ with $1-p^{\alpha-1} \leq \operatorname{mindeg} S$ and $\deg S \leq p^{\alpha-1}\deg(R \bmod p)$, then $\lambda_0^n(S)$ is a polynomial for all $n \geq 1$. Moreover, the polynomial $\lambda_0^n(S)$ is divisible by $z^{p^{\alpha-1}e_0}$ for all $n \geq \lfloor \log_p e_0 \rfloor + \alpha$.*

Proof. Let $s = \operatorname{mindeg} S$, and write $S = z^s T$ (so that $T \in \mathcal{R}_{p^\alpha}[z]$ is a polynomial that is not divisible by z). By Proposition 8, we have

$$\begin{aligned}\lambda_0(S) = \Lambda_0\Big(SR^{p^\alpha - p^{\alpha-1}}\Big) &= \Lambda_0\Big(S(R \bmod p)^{p^\alpha - p^{\alpha-1}}\Big) \\ &= \Lambda_0\Big(z^{s+e_0(p^\alpha-p^{\alpha-1})}TG^{p^\alpha-p^{\alpha-1}}\Big).\end{aligned}$$

Since $1-p^{\alpha-1} \leq s$ and $e_0 \geq 1$, this implies that $\lambda_0(S)$ is a polynomial. Therefore $\lambda_0^n(S)$ is a polynomial for each $n \geq 1$, and $\lambda_0(S)$ is divisible by $z^{f(s)}$, where $f(x) = e_0p^{\alpha-1} + \left\lceil \frac{x-e_0p^{\alpha-1}}{p} \right\rceil$. If $n \geq \lfloor \log_p e_0 \rfloor + \alpha$, then $f^n(x) \geq e_0p^{\alpha-1}$, so $\lambda_0^n(S)$ is divisible by $z^{e_0p^{\alpha-1}}$. □

Finally, we use Proposition 39 to remove the restriction in Theorem 38 that $e_0 \in \{-1,0\}$. We show that if $e_0 \geq 1$ then every application of λ_0 pushes the image into a smaller $\mathcal{R}_{p^\alpha}$-module until we are emulating the map λ_0 for a polynomial G satisfying $\operatorname{mindeg} G = 0$.

Theorem 40. *Let $R \in \mathcal{R}_{p^\alpha}[z]$ be a nonzero polynomial. Factor $(R \bmod p) = cz^{e_0}R_1^{e_1}\cdots R_k^{e_k}$ into irreducibles, and define $G = cR_1^{e_1}\cdots R_k^{e_k}$. Suppose that $e_0 \geq 1$ and $\deg G \geq 1$. Let $\ell = \operatorname{lcm}(\deg R_1,\dots,\deg R_k)$ and let*

$$t = \max\big(\lfloor \log_p e_0 \rfloor + \alpha, \lceil \log_p \max(e_1,\dots,e_k) \rceil + 2(\alpha-1)\big).$$

Let m be the period length of the series expansion of $\frac{1}{G}$. For all $S \in \mathcal{R}_{p^\alpha}[z,z^{-1}]$ with $1-p^{\alpha-1} \leq \operatorname{mindeg} S$ and $\deg S \leq p^{\alpha-1}\deg(R \bmod p)$, the orbit size of S under λ_0 is at most $t+\ell$.

Proof. Since $t \geq \lfloor \log_p e_0 \rfloor + \alpha$, Proposition 39 tells us that $\lambda_0^t(S)$ is divisible by $z^{e_0p^{\alpha-1}}$. Define $T \in \mathcal{R}_{p^\alpha}[z]$ by $\lambda_0^t(S) = z^{e_0p^{\alpha-1}}T$; we claim $\deg T \leq p^{\alpha-1}\deg G$. Since $\deg \lambda_0(S) \leq p^{\alpha-1}\deg(R \bmod p)$, we have

$$\begin{aligned}\deg T &= \deg \lambda_0^t(S) - e_0p^{\alpha-1} \\ &\leq p^{\alpha-1}\deg(R \bmod p) - e_0p^{\alpha-1} \\ &= p^{\alpha-1}\deg G,\end{aligned}$$

as claimed.

For all $T \in \mathcal{R}_{p^\alpha}[z]$ (and in particular for the T satisfying $\lambda_0^t(S) = Tz^{e_0 p^{\alpha-1}}$),

$$\begin{aligned}\lambda_0(Tz^{e_0p^{\alpha-1}}) &= \Lambda_0\Big(Tz^{e_0p^{\alpha-1}}(R \bmod p)^{p^\alpha - p^{\alpha-1}}\Big)\\ &= \Lambda_0\Big(Tc^{p^\alpha-p^{\alpha-1}}z^{e_0p^{\alpha-1}+e_0(p^\alpha-p^{\alpha-1})}G^{p^\alpha-p^{\alpha-1}}\Big)\\ &= \Lambda_0\Big(Tc^{p^\alpha-p^{\alpha-1}}G^{p^\alpha-p^{\alpha-1}}z^{e_0p^\alpha}\Big)\\ &= \Lambda_0\Big(T\,G^{p^\alpha-p^{\alpha-1}}\Big)\,z^{e_0p^{\alpha-1}}.\end{aligned}$$

Accordingly, define $\kappa_0 \colon \mathcal{R}_{p^\alpha}[z] \to \mathcal{R}_{p^\alpha}[z]$ by $\kappa_0(T) = \Lambda_0(T\,G^{p^\alpha-p^{\alpha-1}})$ (where here we can take any lift of G to $\mathcal{R}_{p^\alpha}[z]$), so that $\lambda_0(Tz^{e_0p^{\alpha-1}}) = \kappa_0(T)z^{e_0p^{\alpha-1}}$. Iterating, we have $\lambda_0^\ell(Tz^{e_0p^{\alpha-1}}) = \kappa_0^\ell(T)z^{e_0p^{\alpha-1}}$. The polynomial G satisfies the conditions of Theorem 38. Applying Theorem 38 to κ_0, we have $\kappa_0^{n+\ell}(T) = \kappa_0^n(T)$ for all $n \geq t \geq \lceil \log_p \max(e_1, \ldots, e_k) \rceil + 2(\alpha-1)$ since $\deg T \leq p^{\alpha-1} \deg G$. Therefore

$$\lambda_0^{t+\ell}(S) = \lambda_0^\ell\big(\lambda_0^t(S)\big) = \lambda_0^\ell\Big(Tz^{e_0p^{\alpha-1}}\Big) = \kappa_0^\ell(T)z^{e_0p^{\alpha-1}} = Tz^{e_0p^{\alpha-1}} = \lambda_0^t(S),$$

so the orbit of S under λ_0 contains at most $t + \ell$ elements. □

Next we complement Theorem 38 to allow $\deg(R \bmod p) \geq -1$.

Theorem 41. *Let $R \in z^{-1}\mathcal{R}_{p^\alpha}[z]$ be a nonzero Laurent polynomial such that $\deg(R \bmod p) \in \{-1, 0\}$. Let $e_0 = \operatorname{mindeg}(R \bmod p)$. Define λ_0 on $\mathcal{R}_{p^\alpha}[z, z^{-1}]$ by $\lambda_0(S) = \Lambda_0\Big(SR^{p^\alpha-p^{\alpha-1}}\Big)$. Let $S \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$ with $1 - p^{\alpha-1} \leq \operatorname{mindeg} S$ and $\deg S \leq p^{\alpha-1} \deg(R \bmod p)$.*

- *If $e_0 = -1$, then $\lambda_0^{n+1}(S) = \lambda_0^n(S)$ for all $n \geq 2(\alpha-1)$.*
- *If $e_0 = 0$, then $\lambda_0^{n+1}(S) = \lambda_0^n(S)$ for all $n \geq \alpha - 1$.*

Proof. Let $r := \deg(R \bmod p)$. The assumption that $r \in \{-1, 0\}$ implies $e_0 \in \{-1, 0\}$. If $r = -1$, the only Laurent polynomial S satisfying the constraints is $S = 0$, and the conclusion holds.

Now let $r = 0$, so that we have $(R \bmod p) = bz^{-1} + c$ for some $b, c \in \mathbb{F}_p$ with $c \neq 0$. We consider two cases: $b \neq 0$ so that $e_0 = -1$, and $b = 0$ so that $e_0 = 0$.

Suppose first that $b \neq 0$, and let m be the eventual period length of the coefficient sequence of $\frac{1}{R \bmod p}$. Then

$$\frac{1}{R \bmod p} = \frac{z}{b(1 - (-c/b)z)} = \frac{1}{b}\sum_{n\geq 0}(-c/b)^n z^{n+1}.$$

In particular m divides $p - 1$.

We write $\frac{1}{R^{p^{\alpha-1}}} = \sum_{n\geq 0} a(n)z^n \in \mathcal{R}_{p^\alpha}[\![z]\!]$, and we apply Lemma 32 to the polynomial $T := (zR)^{p^{\alpha-1}} = (zR \bmod p)^{p^{\alpha-1}}$, whose degree is $p^{\alpha-1}$. We deduce that the period of the coefficient sequence of $\frac{1}{T}$ ends with $p^{\alpha-1} - 1$ zeros. As $R^{p^{\alpha-1}} = z^{-p^{\alpha-1}}T$, we can apply Corollary 33 with $i = p^{\alpha-1} - 1$ to conclude that $a(n)_{n\geq 0}$ is eventually periodic, with transient length 1. Moreover, by Corollary 34, the eventual period length of $a(n)_{n\geq 0}$ divides $p^{2(\alpha-1)}m$.

Let $j \in \{1 - p^{\alpha-1}, \ldots, 0\}$, so that kz^j is a monomial in S. Equation (19) still holds, so that $\lambda_0^n(z^j) = \Lambda_0^n\Big(\frac{z^j}{R^{p^{\alpha-1}}}\Big)\,R^{p^{\alpha-1}}$ for all $n \geq 0$. First assume $j = 0$. The series $\frac{z^j}{R^{p^{\alpha-1}}}$ has transient length 1. Applying $2(\alpha-1)$ iterations of Λ_0 produces

a series with transient length at most 1 and eventual period length dividing m. If $j \le -1$ and $n \ge 2(\alpha-1)$, then $\Lambda_0^n\left(\frac{z^j}{R^{p^{\alpha-1}}}\right)$ is periodic with period length dividing m. Since m divides $p-1$ in both cases, we have that the period length divides $p-1$, and therefore p is congruent to 1 modulo the period length. Hence further applications of Λ_0 leave the series fixed. This completes the case $b \neq 0$.

Finally let $b = 0$, so that $(R \bmod p) = c \in \mathbb{F}_p$. Then $\lambda_0^n(S) = c^{n(p^\alpha - p^{\alpha-1})}\Lambda_0^n(S) = \Lambda_0^n(S)$. Using the conditions on S, one verifies that if $n \ge \alpha - 1$ then $\lambda_0^n(S)$ is the constant term of S. □

For the case when $\deg G = 0$, we have a similar result. The proof follows that of Theorem 40 but with an application of the second bullet point of Theorem 41.

Theorem 42. *Let $R \in \mathcal{R}_{p^\alpha}[z]$ be a nonzero polynomial. Suppose that $(R \bmod p) = cz^{e_0}$ with $e_0 \ge 1$. For all $S \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$ with $1 - p^{\alpha-1} \le \operatorname{mindeg} S$ and $\deg S \le p^{\alpha-1}e_0$, the orbit size of S under λ_0 is at most $\alpha - 1$.*

We now have the following general result which includes Theorems 38, 40, 41, and 42.

Corollary 43. *Let $R \in z^{-1}\mathcal{R}_{p^\alpha}[z]$ be a nonzero Laurent polynomial. Factor $(R \bmod p) = cz^{e_0}R_1^{e_1}\cdots R_k^{e_k}$ into irreducibles. Let*

$$t = \max\left(\left\lfloor \log_p \max(e_0, 1)\right\rfloor + \alpha, \left\lceil \log_p \max(e_1, \dots, e_k, 1) + 2(\alpha-1)\right\rceil\right) \tag{21}$$

and $\ell = \operatorname{lcm}(\deg R_1, \dots, \deg R_k)$. Define λ_0 on $\mathcal{R}_{p^\alpha}[z, z^{-1}]$ by $\lambda_0(S) = \Lambda_0\left(SR^{p^\alpha - p^{\alpha-1}}\right)$. For all $S \in \mathcal{R}_{p^\alpha}[z, z^{-1}]$ with $1 - p^{\alpha-1} \le \operatorname{mindeg} S$ and $\deg S \le p^{\alpha-1}\deg(R \bmod p)$, the orbit size of S under λ_0 is at most $t + \ell$.

8. Orbit size under $\lambda_{0,0}$

In this section, we prove Theorems 1 and 2. The last remaining piece is to determine, for each border, how many times we must apply $\lambda_{0,0}$ before we can apply Corollary 43.

Lemma 44. *Let*

$$\begin{aligned} u_\ell &= \left\lfloor \log_p \max\left(p^{\alpha-1}(d - 1 - \deg \pi_{x,0}(Q)), 1\right)\right\rfloor + 1 \\ u_{\mathrm{r}} &= \left\lfloor \log_p \max\left(p^{\alpha-1}(d - 1 - \deg \pi_{x,h}(Q)), 1\right)\right\rfloor + 1 \\ u_{\mathrm{t}} &= \left\lfloor \log_p \max\left(p^{\alpha-1}(h - \deg \pi_{y,d-1}(Q)), 1\right)\right\rfloor + 1. \end{aligned}$$

For all $S \in \operatorname{val}_{p/Q}(\mathcal{V})$, we have

1. $\deg \pi_{x,0}(\lambda_{0,0}^n(S)) \le p^{\alpha-1}\deg \pi_{x,0}(Q)$ *for all $n \ge u_\ell$,*
2. $\deg \pi_{x,p^{\alpha-1}h}(\lambda_{0,0}^n(S)) \le p^{\alpha-1}\deg \pi_{x,h}(Q)$ *for all $n \ge u_{\mathrm{r}}$, and*
3. $\deg \pi_{y,p^{\alpha-1}(d-1)}(\lambda_{0,0}^n(S)) \le p^{\alpha-1}\deg \pi_{y,d-1}(Q)$ *for all $n \ge u_{\mathrm{t}}$.*

Proof. We prove the second statement; the others are similar. Let $R = \pi_{x,h}(Q)$. Since $S \in \operatorname{val}_{p/Q}(\mathcal{V})$, Lemma 19 tells us that $\deg_x S \le p^{\alpha-1}h$ and $\deg_y S \le p^{\alpha-1}(d-1)$. In particular, S satisfies $\deg \pi_{x,p^{\alpha-1}h}(S) \le p^{\alpha-1}(d-1)$, which is $p^{\alpha-1}(d - 1 - \deg \pi_{x,h}(Q))$ away from the target degree $p^{\alpha-1}\deg \pi_{x,h}(Q)$.

Part 2 of Proposition 26 gives

$$\pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,p^{\alpha-1}h}(S)) = \Lambda_0\left(\pi_{x,p^{\alpha-1}h}(S)\cdot(\pi_{x,h}(Q))^{p^\alpha - p^{\alpha-1}}\right).$$

This implies

$$\begin{aligned}\deg \pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)) &\le p^{\alpha-2}(d-1) + \left(p^{\alpha-1} - p^{\alpha-2}\right) \deg \pi_{x,h}(Q) \\ &= p^{\alpha-2}(d-1-\deg \pi_{x,h}(Q)) + p^{\alpha-1} \deg \pi_{x,h}(Q).\end{aligned}$$

Therefore $\deg \pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S))$ is at most $p^{\alpha-2}(d-1-\deg \pi_{x,h}(Q))$ away from the target degree $p^{\alpha-1} \deg \pi_{x,h}(Q)$. Iterating $\lambda_{0,0}$ at most u_{r} times, and then applying $\pi_{x,p^{\alpha-1}h}$, we obtain the target degree. □

We now prove Theorem 2. By Remark 7, the assumption $h \ge 1$ is not restrictive.

Theorem 2. *Let p be a prime, let $\alpha \ge 1$, and let $F = \sum_{n\ge 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!]$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$ such that $h := \deg_x(P \bmod p) \ge 1$. Let $d = \deg_y(P \bmod p)$,*

$$N = \tfrac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd + 1),$$

and

$$u = \left\lfloor \log_p \max\left(\alpha(\deg_x(P \bmod p^\alpha) - h), \alpha(\deg_y(P \bmod p^\alpha) - d) + 1\right)\right\rfloor + 1.$$

Let $Q \in \mathcal{R}_{p^\alpha}[x,y,y^{-1}]$ be a lift of $P/y \bmod p$ which has the same monomial support as $P/y \bmod p$, and define u_ℓ, u_{r}, and u_{t} as in Lemma 44. Then the size of $\ker_p((a(n) \bmod p^\alpha)_{n\ge 0})$ is at most

$$\begin{aligned}&p^N + p^{N-\alpha(\alpha+1)(h+d-1)/2}\mathcal{L}(h,d,d) \\ &\qquad + \max(u_\ell, u_{\mathrm{r}}, u_{\mathrm{t}}) + \left\lceil \log_p \max(h, d-1)\right\rceil + \max(\alpha, 2(\alpha-1)) + \tfrac{p^u-1}{p-1}.\end{aligned}$$

Proof. By Corollary 25, we have

$$|\ker_p((a(n) \bmod p^\alpha)_{n\ge 0})| \le p^N + |\mathrm{orb}_{\Lambda_0}(F \bmod p^\alpha)| + \tfrac{p^u-1}{p-1} - u$$

where N is the dimension of the space $\mathcal{W}$ defined in Equation (8). Equivalently,

$$|\ker_p((a(n) \bmod p^\alpha)_{n\ge 0})| \le p^N + |\mathrm{orb}_{\Lambda_0}(\Lambda_0^u(F \bmod p^\alpha)| + \tfrac{p^u-1}{p-1}.$$

It remains to bound $|\mathrm{orb}_{\Lambda_0}(\Lambda_0^u(F \bmod p^\alpha))| \le |\mathrm{orb}_{\lambda_{0,0}}(\lambda_{0,0}^u(S_0))|$, where S_0 is the initial state. Let $S_u := \lambda_{0,0}^u(S_0)$. By Proposition 23, we have $S_u \in \mathrm{val}_{p/Q}(\mathcal{V})$. We bound $|\mathrm{orb}_{\lambda_{0,0}}(S_u)|$ by emulating $\lambda_{0,0}$ with the appropriate univariate operators λ_0 on the left, right, and top borders of $\mathcal{V}$ and using a crude upper bound for the "interior" $\mathcal{V}^\circ$ defined below. Corollary 28, Lemma 44, and then Corollary 43 will allow us to do this.

For $k \in \{0,1,\dots,\alpha-1\}$, let

$$V_k^\circ := \left\{ \sum_{i=1}^{(k+1)h-1} \sum_{j=\max(-k,-i)}^{(k+1)(d-1)-1} c_{i,j}x^i y^j : c_{i,j} \in D \text{ for each } i,j \right\},$$

and

$$\mathcal{V}^\circ := \{(T_{\alpha-1}, \dots, T_1, T_0) : T_k \in V_k^\circ \text{ for each } k \in \{0,1,\dots,\alpha-1\}\}.$$

We have

$$\begin{aligned}\dim \mathcal{V}^\circ &= \sum_{k=0}^{\alpha-1} \left(((k+1)h-1)\cdot(k+1)(d-1) + \sum_{j=-k}^{-1} ((k+1)h+j) \right) \\ &= \tfrac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd - 3h - 3d + 4) \\ &= N - \tfrac{1}{2}\alpha(\alpha+1)(h+d-1).\end{aligned}$$

We use the following fact. Let U be a finite vector space with basis $\mathcal{B}$. Let $(\mathcal{B}_1, \mathcal{B}_2)$ be a partition of $\mathcal{B}$, and let U_1 and U_2 be the subspaces generated by $\mathcal{B}_1$ and $\mathcal{B}_2$. Let pr_{U_i} denote projection onto U_i. If $f\colon U \to U$ and $\tilde{f}\colon U_1 \to U_1$ are linear transformations satisfying $\mathrm{pr}_{U_1} \circ f = \tilde{f} \circ \mathrm{pr}_{U_1}$, then

$$f(x) = \mathrm{pr}_{U_1}(f(x)) + \mathrm{pr}_{U_2}(f(x)) = \tilde{f}(\mathrm{pr}_{U_1}(x)) + \mathrm{pr}_{U_2}(f(x)),$$

so that $|\mathrm{orb}_f(x)| \le |U_2| \cdot |\mathrm{orb}_{\tilde{f}}(\mathrm{pr}_{U_1}(x))|$ for all $x \in U$.

We apply this fact to $U = \mathcal{V}$, $U_2 = \mathcal{V}^\circ$, and $f\colon \mathcal{V} \to \mathcal{V}$ defined by $f = \mathrm{rep}_{p/Q} \circ \lambda_{0,0} \circ \mathrm{val}_{p/Q}$. The space U_1 is generated by the union of the bases of the three borders. Recall from Section 5 the operators λ_0, defined using one of three Laurent polynomials R by $\lambda_0(S) = \Lambda_0\left(SR^{p^\alpha - p^{\alpha-1}}\right)$. Define the linear transformation $\tilde{f}\colon U_1 \to U_1$ by

- $\tilde{f} \circ \mathrm{pr}_{x,0} = \mathrm{rep}_{p/R} \circ \lambda_0 \circ \mathrm{val}_{p/R} \circ \mathrm{pr}_{x,0}$ where $R = \pi_{x,0}(Q)$,
- $\tilde{f} \circ \mathrm{pr}_{x,h} = \mathrm{rep}_{p/R} \circ \lambda_0 \circ \mathrm{val}_{p/R} \circ \mathrm{pr}_{x,h}$ where $R = \pi_{x,h}(Q)$, and
- $\tilde{f} \circ \mathrm{pr}_{y,d-1} = \mathrm{rep}_{p/R} \circ \lambda_0 \circ \mathrm{val}_{p/R} \circ \mathrm{pr}_{x,d-1}$ where $R = \pi_{y,d-1}(Q)$.

We have defined the images under $\tilde{f}$ of the basis elements x^0y^{d-1} and x^hy^{d-1} twice, but $\tilde{f}$ is well defined by Theorem 27. We claim that $\mathrm{pr}_{U_1} \circ f = \tilde{f} \circ \mathrm{pr}_{U_1}$. We consider each border. For the left border, we show that $\mathrm{pr}_{x,0} \circ f = \tilde{f} \circ \mathrm{pr}_{x,0}$. Corollary 28 gives

$$\begin{aligned}\mathrm{pr}_{x,0} \circ f &= \mathrm{rep}_{p/R} \circ \lambda_0 \circ \pi_{x,0} \circ \mathrm{val}_{p/Q} \\ &= \mathrm{rep}_{p/R} \circ \lambda_0 \circ \mathrm{val}_{p/R} \circ \mathrm{rep}_{p/R} \circ \pi_{x,0} \circ \mathrm{val}_{p/Q}\,.\end{aligned}$$

By Theorem 27, this implies

$$\begin{aligned}\mathrm{pr}_{x,0} \circ f &= \mathrm{rep}_{p/R} \circ \lambda_0 \circ \mathrm{val}_{p/R} \circ \mathrm{pr}_{x,0} \\ &= \tilde{f} \circ \mathrm{pr}_{x,0}\,.\end{aligned}$$

Similarly for the other two borders. The fact in the previous paragraph now implies $|\mathrm{orb}_{\lambda_{0,0}}(S)| = |\mathrm{orb}_f(\mathrm{rep}_{p/Q}(S))| \le |\mathcal{V}^\circ| \cdot |\mathrm{orb}_{\tilde{f}}(\mathrm{pr}_{U_1}(\mathrm{rep}_{p/Q}(S)))|$ for all $S \in \mathrm{val}_{p/Q}(\mathcal{V})$. That is,

$$|\mathrm{orb}_{\lambda_{0,0}}(S)| \le p^{N-\alpha(\alpha+1)(h+d-1)/2} \cdot |\mathrm{orb}_{\tilde{f}}(\mathrm{pr}_{U_1}(\mathrm{rep}_{p/Q}(S)))| \tag{22}$$

for all $S \in \mathrm{val}_{p/Q}(\mathcal{V})$. In particular, this is true for each state $\lambda_{0,0}^n(S_u)$ where $n \ge 0$, since $\lambda_{0,0}^n(S_u) \in \mathrm{val}_{p/Q}(\mathcal{V})$ by Corollary 21.

It remains to bound the orbit size $|\mathrm{orb}_{\tilde{f}}(\mathrm{pr}_{U_1}(\mathrm{rep}_{p/Q}(S_u)))|$. We do this by going from base-$\frac{p}{Q}$ representations back to Laurent polynomials and bounding the orbit sizes of the three projections $\pi_{x,0}(S_u)$, $\pi_{x,p^{\alpha-1}h}(S_u)$, and $\pi_{y,p^{\alpha-1}(d-1)}(S_u)$. The definition of $\tilde{f}$ involves three functions $\tilde{f}_\ell\colon \mathrm{pr}_{x,0}(\mathcal{V}) \to \mathrm{pr}_{x,0}(\mathcal{V})$, $\tilde{f}_\mathrm{r}\colon \mathrm{pr}_{x,h}(\mathcal{V}) \to \mathrm{pr}_{x,h}(\mathcal{V})$, and $\tilde{f}_\mathrm{t}\colon \mathrm{pr}_{y,d-1}(\mathcal{V}) \to \mathrm{pr}_{y,d-1}(\mathcal{V})$. By definition, an orbit under one of

these functions is in bijection with the orbit of the corresponding Laurent polynomial under the respective λ_0 operator.

Corollary 43 allows us to bound an orbit size under λ_0. To satisfy the conditions in Corollary 43, we use Lemma 44 to obtain

$$\begin{aligned}\deg \pi_{x,0}(S_{u+\max(u_\ell,u_\mathrm{r},u_\mathrm{t})}) &\le p^{\alpha-1} \deg \pi_{x,0}(Q)\\ \deg \pi_{x,p^{\alpha-1}h}(S_{u+\max(u_\ell,u_\mathrm{r},u_\mathrm{t})}) &\le p^{\alpha-1} \deg \pi_{x,h}(Q)\\ \deg \pi_{y,p^{\alpha-1}(d-1)}(S_{u+\max(u_\ell,u_\mathrm{r},u_\mathrm{t})}) &\le p^{\alpha-1} \deg \pi_{y,d-1}(Q).\end{aligned}$$

Therefore, the orbits under λ_0, of the three Laurent polynomials obtained by projecting $S_{u+\max(u_\ell,u_\mathrm{r},u_\mathrm{t})}$ onto the three borders, are eventually periodic with transient lengths given by Equation (21). Define t_ℓ, t_r, and t_t to be these transient lengths. We have

$$\begin{aligned}t &:= \max(u_\ell,u_\mathrm{r},u_\mathrm{t}) + \max(t_\ell,t_\mathrm{r},t_\mathrm{t})\\ &\le \max(u_\ell,u_\mathrm{r},u_\mathrm{t}) + \left\lceil \log_p \max(h,d-1)\right\rceil + \max(\alpha, 2(\alpha-1)).\end{aligned}$$

These terms are present in the claimed bound. Set $S_{u+t} := \lambda_{0,0}^{u+t}(S_0)$. We will bound the sizes of the periodic orbits

$$\begin{aligned}\mathrm{orb}_\ell(S_{u+t}) &:= \{\lambda_0^n(\pi_{x,0}(S_{u+t})) : n \ge 0\}\\ \mathrm{orb}_\mathrm{r}(S_{u+t}) &:= \{\lambda_0^n(\pi_{x,p^{\alpha-1}h}(S_{u+t})) : n \ge 0\}\\ \mathrm{orb}_\mathrm{t}(S_{u+t}) &:= \{\lambda_0^n(\pi_{y,p^{\alpha-1}(d-1)}(S_{u+t})) : n \ge 0\}\end{aligned}$$

where again the three operators λ_0 are defined with the respective R. By Corollary 43, we have $|\mathrm{orb}_\ell(S_{u+t})| = \mathrm{lcm}(\sigma)$ for some integer partition $\sigma \in \mathrm{parts}(\deg \pi_{x,0}(Q))$. Similarly, for $|\mathrm{orb}_\mathrm{r}(S_{u+t})|$ and $|\mathrm{orb}_\mathrm{t}(S_{u+t})|$ we obtain two integer partitions in $\mathrm{parts}(\deg \pi_{x,h}(Q))$ and $\mathrm{parts}(\deg \pi_{y,d-1}(Q))$. We have

$$|\mathrm{orb}_{\lambda_{0,0}}(S_{u+t})| \le \mathrm{lcm}(|\mathrm{orb}_\ell(S_{u+t})| \cdot |\mathrm{orb}_\mathrm{r}(S_{u+t})| \cdot |\mathrm{orb}_\mathrm{t}(S_{u+t})|).$$

Therefore $|\mathrm{orb}_{\tilde{f}}(S)| \le \mathcal{L}(h,d,d)$. Finally, Equation (22) gives

$$|\mathrm{orb}_{\lambda_{0,0}}(S_{u+t})| \le p^{N-\alpha(\alpha+1)(h+d-1)/2} \cdot \mathcal{L}(h,d,d)$$

as desired. □

We can now prove Theorem 1.

Theorem 1. *Let p be a prime, let $\alpha \ge 1$, and let $F = \sum_{n\ge 0} a(n)x^n \in \mathbb{Z}_p[\![x]\!] \setminus \{0\}$ be the Furstenberg series associated with a polynomial $P \in \mathbb{Z}_p[x,y]$. Let $h := \deg_x(P \bmod p)$ and $d := \deg_y(P \bmod p)$, and assume $h = \deg_x P$ and $d = \deg_y P$. Then $|\ker_p((a(n) \bmod p^\alpha)_{n\ge 0})|$ is in*

$$(1+o(1))\, p^{\frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha+hd+1)}$$

as any of p, α, h, or d tends to infinity and the others remain constant.

Proof. We use the upper bound from Theorem 2. To bound $\mathcal{L}(h,d,d)$, recall the Landau function $g(n)$ from Section 1. The set of triples of integer partitions of h,d,d gives rise to a subset of integer partitions of $h+2d$. Therefore $\mathcal{L}(h,d,d) \le g(h+2d)$.

By assumption, $\deg_x P = h$ and $\deg_y P = d$. This simplifies the value of u defined in Theorem 2 to $u = 1$. Thus, by Theorem 2, the size of $\ker_p((a(n) \bmod p^\alpha)_{n\ge 0})$ is

at most

$$p^N + p^{N-\alpha(\alpha+1)(h+d-1)/2} g(h+2d) \\ + \max(\alpha, 2(\alpha-1)) + \max(u_\ell, u_\mathrm{r}, u_\mathrm{t}) + \left\lceil \log_p \max(h, d-1) \right\rceil + 1.$$

The expression $\max(\alpha, 2(\alpha-1)) + \max(u_\ell, u_\mathrm{r}, u_\mathrm{t}) + \left\lceil \log_p \max(h, d-1) \right\rceil + 1$ is clearly in $o(1)p^N$ as p, α, h, or d tends to infinity. It remains to show that $p^{N-\alpha(\alpha+1)(h+d-1)/2} g(h+2d)$ is also in $o(1)p^N$. Landau [12] proved that $\log g(n) \sim \sqrt{n \log n}$, that is, $g(n) = e^{(1+\epsilon(n))\sqrt{n \log n}}$, where $\epsilon(n) \to 0$ as $n \to \infty$. It follows that

$$\frac{p^{N-\alpha(\alpha+1)(h+d-1)/2} g(h+2d)}{p^N} = \frac{g(h+2d)}{p^{\alpha(\alpha+1)(h+d-1)/2}} = \frac{e^{(1+\epsilon(h+2d))\sqrt{(h+2d)\log(h+2d)}}}{p^{\alpha(\alpha+1)(h+d-1)/2}},$$

and this tends to 0 as p, α, h, or d tends to infinity and the others remain constant. □

9. Diagonals of rational functions

In this section, we widen our scope from algebraic series to diagonals of multivariate rational functions. Over a field of nonzero characteristic, Furstenberg [10] showed that the diagonal of a multivariate rational function is algebraic. This is a special case of the following result due to Denef and Lipshitz [8, Theorem 6.2 and Remark 6.6].

Theorem 45. *Let p be a prime. Let $P(x_1, \ldots, x_m)$ and $Q(x_1, \ldots, x_m)$ be polynomials in $\mathbb{Z}_p[x_1, \ldots, x_m]$ such that $Q(0, \ldots, 0) \not\equiv 0 \mod p$, and let*

$$F := \mathcal{D}\left(\frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)} \right).$$

Then, for each $\alpha \geq 1$, the coefficient sequence of $F \bmod p^\alpha$ is p-automatic.

The proof of Theorem 45 is constructive [17], and the relevant operators $\lambda_{r,\ldots,r}$ are defined for $S \in \mathcal{R}_{p^\alpha}[x_1, \ldots, x_m]$ by

$$\lambda_{r,\ldots,r}(S) := \Lambda_{r,\ldots,r}\left(S(Q \bmod p^\alpha)^{p^\alpha - p^{\alpha-1}} \right).$$

By Lemma 6, we can replace $Q \bmod p^\alpha$ with a lift of $Q \bmod p$ to $\mathcal{R}_{p^\alpha}[x_1, \ldots, x_m]$ which has the same monomial support as $Q \bmod p$.

The numeration system that we developed in Section 3 for bivariate Laurent polynomials can be adapted to multivariate polynomials. This will allow us to prove Theorem 3.

We begin with a bivariate analogue of Theorem 2. To state it, we extend the function $\mathcal{L}(n_1, n_2, n_3)$ from Section 1 to $\mathcal{L}(n_1, n_2, n_3, n_4)$, defined analogously as the maximum value of $\operatorname{lcm}(\operatorname{lcm}(\sigma_1), \operatorname{lcm}(\sigma_2), \operatorname{lcm}(\sigma_3), \operatorname{lcm}(\sigma_4))$ over integer partitions σ_i of integers in $\{1, 2, \ldots, n_i\}$. The reason for this is that Theorem 45 is symmetric in $x_1, \ldots, x_m$, unlike Theorem 4. This symmetry leads to the appearance of $\mathcal{L}(h, h, d, d)$ in Theorem 46 instead of $\mathcal{L}(h, d, d)$ as in Theorem 2.

Theorem 46. *Let p be a prime, and let $\alpha \geq 1$. Let $P(x, y)$ and $Q(x, y)$ be polynomials in $\mathbb{Z}_p[x, y]$ such that $Q(0, 0) \not\equiv 0 \mod p$. Let*

$$F = \mathcal{D}\left(\frac{P(x, y)}{Q(x, y)} \right),$$

let

$$h = \max(\deg_x(P \bmod p), \deg_x(Q \bmod p))$$
$$d = \max(\deg_y(P \bmod p), \deg_y(Q \bmod p)),$$

and let $N = \frac{1}{6}\alpha(\alpha+1)(2\alpha+1)hd$. *Assume* $h \geq 1$ *and* $d \geq 1$. *Define*

$$\begin{aligned} u = \big\lfloor \log_p \max\big(& \\ & \alpha\,(\max(\deg_x(P \bmod p^\alpha), \deg_x(Q \bmod p^\alpha)) - h), \\ & \alpha\,(\max(\deg_y(P \bmod p^\alpha), \deg_y(Q \bmod p^\alpha)) - d), \\ & 1 \\ \big) \big\rfloor, & \end{aligned}$$

and let

$$u_\ell = \big\lfloor \log_p \max\big(p^{\alpha-1}(d - \deg \pi_{x,0}(Q)), 1\big) \big\rfloor + 1$$
$$u_{\mathrm{r}} = \big\lfloor \log_p \max\big(p^{\alpha-1}(d - \deg \pi_{x,h}(Q)), 1\big) \big\rfloor + 1$$
$$u_{\mathrm{b}} = \big\lfloor \log_p \max\big(p^{\alpha-1}(h - \deg \pi_{y,0}(Q)), 1\big) \big\rfloor + 1$$
$$u_{\mathrm{t}} = \big\lfloor \log_p \max\big(p^{\alpha-1}(h - \deg \pi_{y,d}(Q)), 1\big) \big\rfloor + 1.$$

Write $F = \sum_{n\geq 0} a(n)x^n$. *Then the size of* $\ker_p((a(n) \bmod p^\alpha)_{n\geq 0})$ *is at most*

$$\begin{aligned} & p^N + p^{N-\alpha((\alpha+1)(h+d)-2)/2}\mathcal{L}(h,h,d,d) \\ & \qquad + \max(u_\ell, u_{\mathrm{r}}, u_{\mathrm{b}}, u_{\mathrm{t}}) + \lceil \log_p \max(h,d) \rceil + \max(\alpha, 2(\alpha-1)) + \tfrac{p^u-1}{p-1}. \end{aligned}$$

Consequently, if $h = \max(\deg_x P, \deg_x Q)$ *and* $d = \max(\deg_y P, \deg_y Q)$, *then* $|\ker_p((a(n) \bmod p^\alpha)_{n\geq 0})|$ *is in* $(1+o(1))p^N$ *as any of* p, α, h, *or* d *tends to infinity and the others remain constant.*

We remark that one could further refine the definitions of h and d to obtain more refined bounds; in particular, the bounds on the degrees of the digits of states in the automaton depend more on the degrees of Q than P.

The structure of the proof of Theorem 46 is similar to that of Theorem 2. One difference is that the diagonal in Theorem 4 contains expressions of the form $P(xy, y)$, which led us to shear and to consider the maps $\lambda_{r,0}$ on Laurent polynomials. For general diagonals, the symmetry in x, y means that no shearing is required, and no Laurent polynomials enter the picture. We define the main objects and state the modifications of relevant results used in the proof.

Define h and d as in Theorem 46. Let

$$W_k := \left\{ \sum_{i=0}^{(k+1)h-1} \sum_{j=0}^{(k+1)d-1} c_{i,j}x^i y^j : c_{i,j} \in D \text{ for each } i,j \right\}$$

and

$$V_k := \left\{ \sum_{i=0}^{(k+1)h} \sum_{j=0}^{(k+1)d} c_{i,j}x^i y^j : c_{i,j} \in D \text{ for each } i,j \right\}.$$

Define

$$\mathcal{W} := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in W_k \text{ for each } k \in \{0,1,\ldots,\alpha-1\}\}$$
$$\mathcal{V} := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in V_k \text{ for each } k \in \{0,1,\ldots,\alpha-1\}\}.$$

The dimension of $\mathcal{W}$ is

$$N := \sum_{k=0}^{\alpha-1} (k+1)h \cdot (k+1)d = \tfrac{1}{6}\alpha(\alpha+1)(2\alpha+1)hd.$$

The initial state of the automaton is $S_0 = \left(PQ^{p^{\alpha-1}-1} \bmod p^\alpha\right)$. An analogue of Theorem 17 tells us that every state in the automaton has a base-$\frac{p}{Q \bmod p^\alpha}$ representation. To simplify notation, for the remainder of this section, we refer to this representation as a base-$\frac{p}{Q}$ representation.

To prove Theorem 46, we provide analogues of Lemma 22, Proposition 23, Proposition 26, and Lemma 44. Let

$$h_k = \max(\deg_x(P \bmod p^k), \deg_x(Q \bmod p^k))$$
$$d_k = \max(\deg_y(P \bmod p^k), \deg_y(Q \bmod p^k)).$$

Lemma 47. *The base-$\frac{p}{Q}$ digits T_k of the initial state S_0 satisfy*

$$\deg_x T_k \le (k+1)h_k$$
$$\deg_y T_k \le (k+1)d_k.$$

Proposition 48. *Let S_0 be the initial state, and let $(T_{\alpha-1}, \dots, T_1, T_0) := \mathrm{rep}_{p/Q}(S_0)$. Let*

$$u = \left\lfloor \log_p \max(\alpha(h_{\alpha-1} - h), \alpha(d_{\alpha-1} - d), 1) \right\rfloor + 1.$$

Then, for all $r_1, r_2, \dots, r_u \in \{0, 1, \dots, p-1\}$, we have $\mathrm{rep}_{p/Q}((\lambda_{r_u,0} \circ \cdots \circ \lambda_{r_2,0} \circ \lambda_{r_1,0})(S_0)) \in \mathcal{V}$.

Proposition 49. *We have the following.*

1. *Let $R = \pi_{x,0}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x,y]$,*
$$\pi_{x,0}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,0}(S)).$$
2. *Let $R = \pi_{x,h}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x,y]$ with height at most $p^{\alpha-1}h$,*
$$\pi_{x,p^{\alpha-1}h}(\lambda_{0,0}(S)) = \lambda_0(\pi_{x,p^{\alpha-1}h}(S)).$$
3. *Let $R = \pi_{y,0}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x,y]$,*
$$\pi_{y,0}(\lambda_{0,0}(S)) = \lambda_0(\pi_{y,0}(S)).$$
4. *Let $R = \pi_{y,d}(Q)$. For all $S \in \mathcal{R}_{p^\alpha}[x,y]$ with degree at most $p^{\alpha-1}d$,*
$$\pi_{y,p^{\alpha-1}d}(\lambda_{0,0}(S)) = \lambda_0(\pi_{y,p^{\alpha-1}d}(S)).$$

Lemma 50. *Define u_ℓ, u_r, u_b, and u_t as in Theorem 46. For all $S \in \mathrm{val}_{p/Q}(\mathcal{V})$, we have*

1. $\deg \pi_{x,0}(\lambda_{0,0}^n(S)) \le p^{\alpha-1} \deg \pi_{x,0}(Q)$ *for all $n \ge u_\ell$,*
2. $\deg \pi_{x,p^{\alpha-1}h}(\lambda_{0,0}^n(S)) \le p^{\alpha-1} \deg \pi_{x,h}(Q)$ *for all $n \ge u_\mathrm{r}$,*
3. $\deg \pi_{y,0}(\lambda_{0,0}^n(S)) \le p^{\alpha-1} \deg \pi_{y,0}(Q)$ *for all $n \ge u_\mathrm{b}$, and*
4. $\deg \pi_{y,p^{\alpha-1}d}(\lambda_{0,0}^n(S)) \le p^{\alpha-1} \deg \pi_{y,d}(Q)$ *for all $n \ge u_\mathrm{t}$.*

Define

$$V_k^\circ := \left\{ \sum_{i=1}^{(k+1)h-1} \sum_{j=1}^{(k+1)d-1} c_{i,j} x^i y^j : c_{i,j} \in D \text{ for each } i,j \right\},$$

and define

$$\mathcal{V}^\circ := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in V_k^\circ \text{ for each } k \in \{0, 1, \ldots, \alpha-1\}\}.$$

We have

$$\begin{aligned}\dim \mathcal{V}^\circ &= \tfrac{1}{6}\alpha(2\alpha^2 hd + 3\alpha(hd - h - d) + hd - 3h - 3d + 6) \\ &= N - \tfrac{1}{2}\alpha((\alpha+1)(h+d) - 2).\end{aligned}$$

With Lemma 47, Proposition 48, Proposition 49, and Lemma 50, one can follow the proof of Theorem 2 to give a proof of Theorem 46.

Finally, we prove Theorem 3.

Theorem 3. *Let p be a prime, let $\alpha \geq 1$, and let*

$$F := \mathcal{D}\left(\frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)}\right)$$

where $P(x_1, \ldots, x_m)$ and $Q(x_1, \ldots, x_m)$ are polynomials in $\mathbb{Z}_p[x_1, \ldots, x_m]$ such that $Q(0, \ldots, 0) \not\equiv 0 \mod p$ and $m \geq 2$. Write $F = \sum_{n \geq 0} a(n)x^n$. Let $h_i = \max(\deg_{x_i}(P \bmod p), \deg_{x_i}(Q \bmod p))$, and assume that $h_i \geq 1$ for each i. Let $M = \sum_{k=0}^{\alpha-1} \prod_{i=1}^{m}((k+1)h_i + 1)$; then

$$|\ker_p((a(n) \bmod p^\alpha)_{n \geq 0})| \leq p^M.$$

Proof. The proof of the bound is similar to the proof of Corollary 24. Namely, let

$$V_k := \left\{S \in D[x_1, \ldots, x_m] : \deg_{x_i} S \leq (k+1)h_i \text{ for each } i\right\}$$

and

$$\mathcal{V} := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in V_k \text{ for each } k \in \{0, 1, \ldots, \alpha-1\}\}.$$

Then we have

$$\dim \mathcal{V} = \sum_{k=0}^{\alpha-1} \prod_{i=1}^{m}((k+1)h_i + 1) = M.$$

By Lemma 47, the initial state belongs to $\mathcal{V}$. By a version of Corollary 21, we have $\lambda_{r,0}(\mathrm{val}_{p/Q}(\mathcal{V})) \subseteq \mathrm{val}_{p/Q}(\mathcal{V})$. The statement follows. □

Remark 51. For $m \geq 3$, we cannot do better without a multivariate version of the results of Section 7, in particular Corollary 43. For example, let $m = 3$. One can modify the beginning of the proof of Theorem 2 to bound $|\mathrm{orb}_{\lambda_{0,0,0}}(S_0)|$ using $p^{\dim \mathcal{V}^\circ}$ and six bivariate operators $\lambda_{0,0}$, where

$$V_k^\circ := \left\{S \in D[x_1, x_2, x_3] : 1 \leq \mathrm{mindeg}_{x_i} S \text{ and } \deg_{x_i} S \leq (k+1)h_i - 2 \text{ for each } i\right\}$$

and

$$\mathcal{V}^\circ := \{(T_{\alpha-1}, \ldots, T_1, T_0) : T_k \in V_k^\circ \text{ for each } k \in \{0, 1, \ldots, \alpha-1\}\}.$$

We have

$$\dim \mathcal{V}^\circ = \sum_{k=0}^{\alpha-1} \prod_{i=1}^{3}((k+1)h_i - 2).$$

By Theorem 46, the orbit size of the projection of the initial state onto one of the six borders under the relevant operator $\lambda_{0,0}$ is in $(1 + o(1))p^{\frac{1}{6}\alpha(\alpha+1)(2\alpha+1)h_i h_j}$ for the appropriate i and j where $i \neq j$. However, this is too large relative to the size of $\mathcal{W}$, defined by

$$W_k := \left\{S \in D[x_1, x_2, x_3] : \deg_{x_i} S \leq (k+1)h_i - 1 \text{ for each } i\right\}$$

and

$$\mathcal{W} := \{(T_{\alpha-1}, \dots, T_1, T_0) : T_k \in W_k \text{ for each } k \in \{0, 1, \dots, \alpha-1\}\}.$$

Namely, we have

$$N := \dim \mathcal{W} = \sum_{k=0}^{\alpha-1} \prod_{i=1}^{3} (k+1)h_i = \tfrac{1}{4}\alpha^2(\alpha+1)^2 h_1 h_2 h_3.$$

Let $S_0 = \left(PQ^{p^{\alpha-1}-1} \bmod p^\alpha\right)$. If $r > 0$, then a version of Corollary 21 gives $\operatorname{rep}_{p/Q}(\lambda_{r,r,r}(S_0)) \in \mathcal{W}$. It remains to consider $|\operatorname{orb}_{\lambda_{0,0,0}}(S_0)|$. The ratio of the orbit size of S_0 under this $\lambda_{0,0,0}$ to the size of $\mathcal{W}$ is in

$$\frac{p^{\dim \mathcal{V}^\circ} \cdot (1+o(1)) p^{\frac{1}{6}\alpha(\alpha+1)(2\alpha+1)(2h_1h_2+2h_1h_3+2h_2h_3)}}{p^{\frac{1}{4}\alpha^2(\alpha+1)^2 h_1 h_2 h_3}} = (1+o(1)) p^{2\alpha(\alpha+1)(h_1+h_2+h_3)-8\alpha},$$

which clearly is not in $o(1)$ as p, α, h_1, h_2, or h_3 tends to infinity.

10. Compatibility of automata

Finally, we return to the setting of Theorems 1 and 2, where F is the Furstenberg series associated with a polynomial P. When we vary α, the automata $\mathcal{M}_{p^\alpha}$ support an inverse limit, as described by the authors [18]. In this section, we show that the base-$\frac{p}{Q}$ representations of states in $\mathcal{M}_{p^{\alpha+1}}$ project onto those of states in $\mathcal{M}_{p^\alpha}$. This gives a new proof of the existence of the inverse limit, with explicit descriptions of the states as sequences of base-$\frac{p}{Q}$ digits. We begin with an example.

Example 52. Let P be the polynomial in Examples 13 and 16 with $p = 2$, but now let $\alpha = 2$. We consider the set of states $\mathcal{M}_4$ in the automaton generating the sequence $(a(n) \bmod 4)_{n\geq 0}$. Let $S_0 = \left(y\frac{\partial P}{\partial y}\,(P/y) \bmod 4\right)$. The orbit of S_0 under $\lambda_{0,0}$ begins

$$\begin{aligned}\operatorname{rep}_{p/Q}(S_0) &= \left(x^2y^3 + (x^2+x)y^2 + x^2y,\ (x+1)y\right)\\ \operatorname{rep}_{p/Q}(\lambda_{0,0}(S_0)) &= \left(x^2y^2 + (x^2+x)y + x^2,\ xy + x\right).\end{aligned}$$

For each of these two states, the two digits T_0 and T_1 are the same as for the corresponding states modulo 8 in Examples 13 and 16.

The following notation allows us to simultaneously work with Cartier operators defined on different rings.

Notation. Define $\hat{Q} \in \mathbb{Z}_p[x, y, y^{-1}]$ to be a lift of $P/y \bmod p$ which has the same monomial support as $P/y \bmod p$. For all $\alpha \geq 1$ and $S \in \mathcal{R}_{p^\alpha}[x, y, y^{-1}]$, define

$$\lambda_{r,0}^{(\alpha)}(S) := \Lambda_{r,0}\left(S\,(\hat{Q} \bmod p^\alpha)^{p^\alpha - p^{\alpha-1}}\right).$$

For the remainder of this section, for $\alpha \geq 1$, we use the convention of writing $\operatorname{rep}_{p/\hat{Q}}(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)}))$ as shorthand for $\operatorname{rep}_{p/(\hat{Q} \bmod p^\alpha)}(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)}))$.

Theorem 53. *Let $\beta \in \{1, 2, \dots, \alpha\}$. Let $S^{(\beta)} \in \mathcal{M}_{p^\beta}$ and $S^{(\alpha)} \in \mathcal{M}_{p^\alpha}$ such that the first β digits of $\operatorname{rep}_{p/\hat{Q}}(S^{(\alpha)})$ agree with $\operatorname{rep}_{p/\hat{Q}}(S^{(\beta)})$. Then the first β digits of $\operatorname{rep}_{p/\hat{Q}}(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)}))$ agree with $\operatorname{rep}_{p/\hat{Q}}(\lambda_{r,0}^{(\beta)}(S^{(\beta)}))$.*

Proof. Let $\operatorname{rep}_{p/\hat{Q}}(S^{(\alpha)}) = (T_{\alpha-1}, \ldots, T_1, T_0)$; by assumption,

$$S^{(\beta)} = \left(\left(T_0 + T_1 \tfrac{p}{\hat{Q}} + \cdots + T_{\beta-1} (\tfrac{p}{\hat{Q}})^{\beta-1} \right) \hat{Q}^{p^{\beta-1}-1} \bmod p^\beta \right).$$

By Theorem 17, $\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})$ has a base-$\frac{p}{\hat{Q}}$ representation. Let T'_m be the mth base-$\frac{p}{\hat{Q}}$ digit of $\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})$. We show that $T'_0, T'_1, \ldots, T'_{\beta-1}$ are defined from $T_0, T_1, \ldots, T_{\beta-1}$ and $(\hat{Q} \bmod p^\beta)$ in the same way as the digits of $\lambda_{r,0}^{(\beta)}(S^{(\beta)})$. This implies the statement of the theorem.

We use the proof of Theorem 14. Define $U_{k,j}$ as in Equation (7). From the proof of Theorem 14, the mth unnormalized digit of $\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})$ is $\sum_{k=0}^{m} U_{k,m-k}$. If we can show that the mth unnormalized digits of $\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})$ and $\lambda_{r,0}^{(\beta)}(S^{(\beta)})$ agree, then their first β normalized digits also agree.

For $m = 0$, we have $T'_0 = U_{0,0} \equiv \Lambda_{r,0}\left(T_k \hat{Q}^{-1}\right) \hat{Q} \mod p$. Therefore the 0th digits satisfy $\operatorname{dig}_0(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})) = \operatorname{dig}_0(\lambda_{r,0}^{(\beta)}(S^{(\beta)}))$.

Inductively, let $m \in \{1, 2, \ldots, \beta-2\}$ and suppose that each $U_{k,j}$ for $k+j < m$ depends only on $T_0, T_1, \ldots, T_{m-1}$ and $(\hat{Q} \bmod p^m)$. This implies that $\operatorname{dig}_k(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})) = \operatorname{dig}_k(\lambda_{r,0}^{(\beta)}(S^{(\beta)}))$ for $k \in \{0, 1, \ldots, m-1\}$. We will show that each $U_{k,j}$ for $k+j = m$ depends only $T_0, T_1, \ldots, T_m$ and $(\hat{Q} \bmod p^{m+1})$; this will imply $\operatorname{dig}_m(\lambda_{r,0}^{(\alpha)}(S^{(\alpha)})) = \operatorname{dig}_m(\lambda_{r,0}^{(\beta)}(S^{(\beta)}))$. Assume $k + j = m$. By the construction of $U_{k,j}$ in the proof of Theorem 14, we have

$$\Lambda_{r,0}\left(T_k \hat{Q}^{-k-1}\right) \hat{Q}^{k+j+1} \equiv U_{k,0}\hat{Q}^j + \cdots + p^{j-1}U_{k,j-1}\hat{Q} + p^j U_{k,j} \mod p^{j+1}.$$

Therefore

$$\frac{\Lambda_{r,0}\left(T_k \hat{Q}^{-k-1}\right) \hat{Q}^{k+j+1} - \left(U_{k,0}\hat{Q}^j + \cdots + p^{j-1}U_{k,j-1}\hat{Q}\right)}{p^j} \equiv U_{k,j} \mod p.$$

The left side depends only on $T_0, T_1, \ldots, T_m$ and $(\hat{Q} \bmod p^{m+1})$. □

Corollary 54. *Let p be a prime. The inverse limit of the automata $\mathcal{M}_{p^\alpha}$ exists, and each state in the inverse limit is identified with an infinite sequence of base-$\frac{p}{\hat{Q}}$ digits.*

Proof. Let $\alpha \geq 1$, and let $\beta \in \{1, 2, \ldots, \alpha\}$. Denote the initial states in $\mathcal{M}_{p^\beta}$ and $\mathcal{M}_{p^\alpha}$ by $S_0^{(\beta)}$ and $S_0^{(\alpha)}$. We will show that for each $k \in \{0, 1, \ldots, \beta-1\}$, we have $\operatorname{dig}_k(S_0^{(\alpha)}) = \operatorname{dig}_k(S_0^{(\beta)})$. Then Theorem 53 tells us that for $n \geq 0$ and $r_1, r_2, \ldots, r_n \in \{0, 1, \ldots, p-1\}$, the first β digits of $\operatorname{rep}_{p/\hat{Q}}((\lambda_{r_n,0}^{(\alpha)} \circ \cdots \circ \lambda_{r_2,0}^{(\alpha)} \circ \lambda_{r_1,0}^{(\alpha)})(S_0^{(\alpha)}))$ agree with $\operatorname{rep}_{p/\hat{Q}}((\lambda_{r_n,0}^{(\beta)} \circ \cdots \circ \lambda_{r_2,0}^{(\beta)} \circ \lambda_{r_1,0}^{(\beta)})(S_0^{(\beta)}))$. This allows us to define $\pi_{\alpha,\beta} \colon \mathcal{M}_{p^\alpha} \to \mathcal{M}_{p^\beta}$ as follows. Identifying a state S with $\operatorname{rep}_{p/\hat{Q}}(S)$, define $\pi_{\alpha,\beta}((T_{\alpha-1}, \ldots, T_1, T_0)) = (T_{\beta-1}, \ldots, T_1, T_0)$. It is clear that if there is a state transition from S to S' in $\mathcal{M}_{p^\alpha}$ then there is a transition labeled r from $\pi_{\alpha,\beta}(S)$ to $\pi_{\alpha,\beta}(S')$ in $\mathcal{M}_{p^\beta}$. Finally, if $\gamma \leq \beta \leq \alpha$, we have $\pi_{\alpha,\gamma} = \pi_{\beta,\gamma} \circ \pi_{\alpha,\beta}$. This means that we have a well defined inverse limit $\varprojlim \mathcal{M}_{p^\alpha}$ whose states have the claimed structure.

It remains to show that for each $k \in \{0, 1, \ldots, \beta-1\}$, we have $\operatorname{dig}_k(S_0^{(\alpha)}) = \operatorname{dig}_k(S_0^{(\beta)})$. From the proof of Theorem 17, the 0th digit of $S_0^{(\alpha)}$ is $T_0 = \left(y \frac{\partial P}{\partial y} \bmod p\right)$,

and this is independent of α. Recursively, for $k \geq 1$, the kth digit of $S_0^{(\alpha)}$ is

$$\frac{y\frac{\partial P}{\partial y} \cdot \frac{\hat{Q} \bmod p^\alpha}{P/y} - T_0 - T_1\left(\frac{p}{\hat{Q} \bmod p^\alpha}\right) - \cdots - T_{k-1}\left(\frac{p}{\hat{Q} \bmod p^\alpha}\right)^{k-1}}{p^k}(\hat{Q} \bmod p^\alpha)^k \bmod p,$$

similarly for the kth digit of $S_0^{(\beta)}$. By definition of $\hat{Q}$, the numerators of these expressions are congruent to each other modulo p^{k+1}. Dividing by p^k, they are congruent modulo p. Therefore these expressions are congruent modulo p, so $\mathrm{dig}_k(S_0^{(\alpha)}) = \mathrm{dig}_k(S_0^{(\beta)})$. □

Appendix: Explicit automaton sizes

The tables in this appendix contain polynomials $P \in \mathcal{R}_{p^\alpha}[x, y]$, found through systematic searches, whose Furstenberg series achieve maximum automaton size or maximum orbit size under $\lambda_{0,0}$. By definition, $P(0, 0) = 0$ and $\frac{\partial P}{\partial y}(0, 0) \not\equiv 0 \mod p$; for simplicity, we require that the coefficient of x^0y^1 in P is 1. All polynomials listed happen to satisfy $h = \deg_x P$ and $d = \deg_y P$, so the value of u in Theorem 2 is always $u = 1$. The automata were computed with the Mathematica package IntegerSequences [13, 14].

Table 1 lists the maximum unminimized automaton size for several values of p, α, h, and d, along with one polynomial that achieves this size and the value of the bound in Theorem 2.

Table 2 contains data on maximal orbit sizes under $\lambda_{0,0}$. For these searches, we assume that the coefficients in P belong to $\{0, 1, \ldots, p-1\}$ to make the search space more accessible. In practice, this restriction does not seem to be consequential. For $p^\alpha \in \{4, 8\}$, $d = 1$, and $h \leq 4$, only one polynomial with a coefficient outside this range results in a larger orbit size, namely $(2x + 1)y + x$, which yields orbit size 3 modulo 4 and also 3 modulo 8. For $p^\alpha \in \{4, 8\}$, $d = 2$, and $h \leq 2$, no polynomials result in a larger orbit size.

Surprisingly, all but one of the polynomials that maximize the orbit size for $p^\alpha = 4$ in Table 2 also maximize the orbit size for $p^\alpha = 8$. These polynomials are therefore good candidates for obtaining maximal orbit sizes for larger values of α. For example, let $P = x^2y^2 + (x^2 + x + 1)y + x^2$. For each $\alpha \in \{1, 2, \ldots, 14\}$, the transient length under $\lambda_{0,0}$ is $\alpha + 1$ and the eventual period length is $2^{\alpha+1}$, leading one to conjecture that the orbit size is exactly $2^{\alpha+1} + \alpha + 1$ for all $\alpha \geq 1$. This perhaps suggests the true growth rate, indicating a possible direction for future work.

$p^\alpha = 4$:

h	d	P	aut. size	p^N
1	1	$(x+1)y+x$	6	16
2	1	$(3x^2+x+1)y+x^2$	18	512
3	1	$(x^3+x+1)y+x^3$	70	16384
4	1	$(3x^4+x+1)y+x^4+x$	189	524288
1	2	$(x+2)y^2+(x+1)y+x$	18	512
2	2	$(x^2+x+3)y^2+(2x^2+x+1)y+x$	222	524288
3	2	$(x^3+x^2+1)y^2+(x^3+1)y+x$	4826	536870912

$p^\alpha = 8$:

h	d	P	aut. size	p^N
1	1	$(x+1)y+x$	10	1024
2	1	$(3x^2+x+1)y+x^2+x$	61	16777216
3	1	$(x^3+x+1)y+x^3$	246	274877906944
1	2	$(x+2)y^2+(5x+1)y+x$	56	16777216
2	2	$(x^2+x+3)y^2+(x^2+2x+1)y+x^2$	2571	4503599627370496

$p^\alpha = 9$:

h	d	P	aut. size	p^N
1	1	$(4x+1)y+x$	14	81
2	1	$(2x^2+7x+1)y+x^2+x$	123	19683
3	1	$(4x^3+2x+1)y+x^3$	562	4782969
1	2	$(x+4)y^2+y+x$	171	19683
2	2	$(x^2+x+5)y^2+(x^2+1)y+x$	11073	1162261467

TABLE 1. Polynomials in $\mathcal{R}_{p^\alpha}[x,y]$ achieving the maximum unminimized automaton size for given values of p, α, h, and d. The value of N in the final column is $N = \frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha+hd+1)$ from Theorem 2.

$p^\alpha = 4$:

h	d	P	orbit size	bound
1	1	$y + x$	2	9
2	1	$y + x^2 + x$	4	135
3	1	$y + x^3 + x^2$	4	3080
4	1	$y + x^4 + x$	5	65545
5	1	$(x^5 + x + 1)y + x$	7	1572874
6	1	$(x^5 + x + 1)y + x^6 + x$	8	25165834
7	1	$(x^7 + x^6 + x^2 + x + 1)y + x$	13	805306378
8	1	$(x^8 + x^3 + 1)y + x$	16	1.61×10^{10}
9	1	$(x^9 + x^2 + 1)y + x$	21	3.43×10^{11}
10	1	$(x^{10} + x^6 + x^3 + x^2 + 1)y + x$	31	8.24×10^{12}
1	2	$xy^2 + (x + 1)y + x$	4	133
2	2	$x^2y^2 + (x^2 + x + 1)y + x^2$	11	2097159
3	2	$(x^3 + x + 1)y^2 + (x^3 + 1)y + x^3$	25	1.03×10^{11}
4	2	$(x^4 + x^2 + x)y^2 + (x^4 + x + 1)y + x^4$	50	1.68×10^{15}
5	2	$(x^5 + x^3 + 1)y^2 + (x^5 + x + 1)y + x$	121	4.61×10^{19}
6	2	$(x^6 + x^4 + x)y^2 + (x^5 + x + 1)y + x^3$	122	7.55×10^{23}
7	2	$(x^7 + x + 1)y^2 + (x^7 + x^6 + x^5 + x + 1)y + x$	337	1.73×10^{28}

$p^\alpha = 8$:

h	d	P	orbit size	bound
1	1	$y + x$	2	4104
2	1	$y + x^2 + x$	5	1.37×10^{11}
3	1	$y + x^3 + x^2$	5	3.45×10^{18}
4	1	$y + x^4 + x$	6	7.73×10^{25}
5	1	$(x^5 + x + 1)y + x$	8	1.94×10^{33}
6	1	$(x^5 + x + 1)y + x^6$	9	3.26×10^{40}
7	1	$(x^7 + x^6 + x^2 + x + 1)y + x$	14	1.09×10^{48}
8	1	$(x^8 + x^3 + 1)y + x$	17	2.29×10^{55}
9	1	$(x^9 + x^2 + 1)y + x$	22	5.14×10^{62}
10	1	$(x^{10} + x^6 + x^3 + x^2 + 1)y + x$	32	1.29×10^{70}
1	2	$xy^2 + (x + 1)y + x$	5	1.37×10^{11}
2	2	$x^2y^2 + (x^2 + x + 1)y + x^2$	20	1.01×10^{31}
3	2	$(x^3 + x + 1)y^2 + (x^3 + 1)y + x^3$	50	2.24×10^{51}
4	2	$(x^4 + x^2 + x)y^2 + (x^4 + x + 1)y + x^4$	99	1.65×10^{71}
5	2	$(x^5 + x^3 + 1)y^2 + (x^5 + x + 1)y + x$	242	2.03×10^{91}
6	2	$(x^6 + x^4 + x)y^2 + (x^5 + x + 1)y + x^3$	243	1.50×10^{111}
7	2	$(x^7 + x + 1)y^2 + (x^7 + x^6 + x^5 + x + 1)y + x$	674	1.55×10^{131}

$p^\alpha = 9$:

h	d	P	orbit size	bound
1	1	$y + x$	2	14
2	1	$y + x^2 + x$	3	1464
3	1	$y + x^3 + x$	4	177154
4	1	$(2x^4 + x + 1)y + x$	5	19131884
5	1	$(x^5 + 2x^2 + 1)y + x$	7	2324522942
6	1	$(x^5 + 2x^2 + 1)y + x^6$	8	1.88×10^{11}
1	2	$xy^2 + y + x$	4	1463
2	2	$(x^2 + x + 1)y^2 + y + x^2 + x$	20	6973568808
3	2	$(x^3 + x^2 + x + 2)y^2 + (x + 1)y + x^3 + x$	57	1.00×10^{17}
4	2	$(x^3 + 2x + 1)y^2 + (x^4 + 1)y + x$	218	4.78×10^{23}

TABLE 2. Polynomials with coefficients in $\{0, 1, \ldots, p-1\}$ for which the initial state achieves the maximum orbit size under $\lambda_{0,0}$ for given values of p, α, h, and d. The final column contains the value of $p^{N-\alpha(\alpha+1)(h+d-1)/2}\mathcal{L}(h,d,d) + \lfloor \log_p \max(p^{\alpha-1}h, p^{\alpha-1}(d-1)) \rfloor + 1 + \lceil \log_p \max(h, d-1) \rceil + \max(\alpha, 2(\alpha-1)) + 1$ from Theorem 2.

References

[1] Boris Adamczewski, Alin Bostan, and Xavier Caruso, A sharper multivariate Christol's theorem with applications to diagonals and Hadamard products, `https://arxiv.org/abs/2306.02640`.

[2] Jean-Paul Allouche and Jeffrey Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press (2003).

[3] Frits Beukers, p-linear schemes for sequences modulo p^r, *Indagationes Mathematicae* **35** (2024) 698–707.

[4] Andrew Bridy, Automatic sequences and curves over finite fields, *Algebra & Number Theory* **11** (2017) 685–712.

[5] Gilles Christol, Ensembles presque périodiques k-reconnaissables, *Theoretical Computer Science* **9** (1979) 141–145.

[6] Gilles Christol, Fonctions et éléments algébriques, *Pacific Journal of Mathematics* **125** (1986) 1–37.

[7] Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy, Suites algébriques, automates et substitutions, *Bulletin de la Société Mathématique de France* **108** (1980) 401–419.

[8] Jan Denef and Leonard Lipshitz, Algebraic power series and diagonals, *Journal of Number Theory* **26** (1987) 46–67.

[9] Howard T. Engstrom, On sequences defined by linear recurrence relations, *Transactions of the American Mathematical Society* **33** (1931) 210–218.

[10] Harry Furstenberg, Algebraic functions over finite fields, *Journal of Algebra* **7** (1967) 271–277.

[11] Joel A. Henningsen and Armin Straub, Generalized Lucas congruences and linear p-schemes, *Advances in Applied Mathematics* **141** (2022) 102409.

[12] Edmund Landau, Über die Maximalordung der Permutation gegbenen Grades, *Archiv der Mathematik und Physik* Series 3, **5** (1903) 92–103.

[13] Eric Rowland, IntegerSequences, `https://github.com/ericrowland/IntegerSequences`.

[14] Eric Rowland, IntegerSequences: a package for computing with k-regular sequences, International Congress on Mathematical Software, *Lecture Notes in Computer Science* **10931** (2018) 414–421.

[15] Eric Rowland, What is an automatic sequence?, *Notices of the American Mathematical Society* **62** (2015) 274–276.

[16] Eric Rowland, Manon Stipulanti, and Reem Yassawi, Algebraic power series and their automatic complexity I: finite fields, `https://arxiv.org/abs/2308.10977`.

[17] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *Journal de Théorie des Nombres de Bordeaux* **27** (2015) 245–288.

[18] Eric Rowland and Reem Yassawi, Profinite automata, *Advances in Applied Mathematics* **85** (2017) 60–83.

[19] Eric Rowland and Doron Zeilberger, A case study in meta-automation: automatic generation of congruence automata for combinatorial sequences, *Journal of Difference Equations and Applications* **20** (2014) 973–988.

[20] Neil Sloane et al., The On-Line Encyclopedia of Integer Sequences, `https://oeis.org`.

[21] Armin Straub, On congruence schemes for constant terms and their applications, *Research in Number Theory* **8** (2022) #42.

[22] Światomir Ząbek, Sur la périodicité modulo m des suites de nombres $\binom{n}{k}$, *Annales Universitatis Mariae Curie-Skłodowska, sectio A – Mathematica* **10** (1956) 37–47.

Department of Mathematics, Hofstra University, Hempstead, NY, USA

School of Mathematical Sciences, Queen Mary University of London, Mile End Road, London E1 4NS, UK