Sparse Automatic Sets

by

Seda Albayrak

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2020

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner: Michel Rigo
Professor, Department of Mathematics,
University of Liege

Supervisor: Jason P. Bell
Professor, Department of Pure Mathematics,
University of Waterloo

Internal Member(s): Kevin Hare
Professor, Department of Pure Mathematics,
University of Waterloo

Wentang Kuo
Associate Professor, Department of Pure Mathematics,
University of Waterloo

Internal-External Member: Penny Haxell
Professor, Department of Combinatorics and Optimization,
University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

Seda Albayrak is the author for the material in Chapters 1–7, and the material in Chapter 6 was written as part of collaboration with Jason Bell; the material in Chapter 6 has been submitted for publication and is available on the arXiv at arXiv:1909.02942. The material in Chapters 2 and 3 is expository and the author does not take credit for the results in these chapters. Material in Chapters 4 and 5 is new and was written by the author with some useful ideas and additions suggested to her by Jason Bell.

All of the research appearing in this thesis was conducted at the University of Waterloo by Seda Albayrak and, in the case of the material from Chapter 6, by Seda Albayrak and Jason Bell. As is the case with mathematical work, all contributions in joint work are assumed to be equal and order of authors on associated manuscripts is determined using alphabetical order of surnames.

Abstract

The theory of automatic sets and sequences arises naturally in many different areas of mathematics, notably in the study of algebraic power series in positive characteristic, due to work of Christol [14, 15], and in Derksen's [18] classification of zero sets for sequences satisfying a linear recurrence over fields of positive characteristic.

A fundamental dichotomy for automatic sets shows that they are either sparse, having counting functions that grow relatively slowly, or they are not sparse, in which case their counting functions grow reasonably fast. While this dichotomy has been known to hold for some time, there has not—to this point in time—been a systematic study of the algebraic and number theoretic properties of sparse automatic sets.

This thesis rectifies this situation and gives multiple results dealing specifically with sparse automatic sets. In particular, we give a stronger version of a classical result of Cobham for automatic sets where one now specializes to sparse automatic sets; we then prove that a conjecture of Erdős and Turán [19] holds for automatic sets, again using the theory of sparseness; finally, we give a refinement of a classical result of Christol where we consider algebraic power series whose support set is a sparse automatic set.

Acknowledgments

I would like to thank my supervisor Jason P. Bell for his support during my Ph.D. studies and for carefully reading my thesis.

I would like to thank Professors Kevin Hare, Penny Haxell, Wentang Kuo, and Michel Rigo for being on the Examining Committee for this thesis, and thank all the committee members for their comments both before and during the defence of my thesis.

I am most thankful to Zeyno Beşikçi, Aslı Eraltan and Ufuk Yazkan for their support during my undergraduate years. It is also a pleasure to thank my friends Abrez & Güneş, Becca & Josh, Ekin, and Jess for their support during my hard times and for being with me all the time. Also, I am thankful to Kübra, Ertan, and Jordan for their great friendship, support and guidance.

Dedication

This is dedicated to my father Kenan Albayrak.

Table of Contents

List of Figures

Chapter 1

Introduction

This thesis deals with sparse automatic sets and their algebraic and number theoretic properties. For the reader's convenience we shall cover a lot of the fundamental background from automata theory needed to read the results in this thesis in Chapter 2, but one can intuitively view automatic sets as being sets S of natural numbers that have an associated fixed natural number k and for which the decision of whether a number n is in the set S or not is done so by taking the base-k expansion of n and feeding it into a machine which then makes the decision about membership in the set S.

These sets are part of a larger universe of *computable* subsets of natural numbers and they are the least complex of the computable sets in a hierarchy first given by Chomsky [13].

As it turns out, there is a striking gap in the possible growth types of automatic sets S: $\pi_S(x) = |\{n \leq x\colon n \in S\}|$ is either poly-logarithmically bounded (i.e., $\pi_S(x) = \mathrm{O}((\log x)^d)$ for some $d \geq 1$) or it grows at least like a fractional power of x (i.e., there exists $\alpha > 0$ such that $\pi_S(x) \geq x^\alpha$ for x sufficiently large).

Automatic sets for which the growth function is poly-logarithmically bounded are called *sparse* and they have been shown to arise in many different contexts. We give some of the more important examples. Derksen's positive characteristic version of the Skolem-Mahler-Lech theorem [18] (see also [10, Chap. 11]) makes use of such sets. In [18], it is shown that the zero set of a linearly recurrent sequence over a field of characteristic $p > 0$ is a finite union of arithmetic progressions augmented by a sparse p-automatic set.

Another relevant work is Kedlaya's description of the algebraic closure of global function fields in positive characteristic. In [28, 29], he extends earlier work of Christol [2, Theorem

12.2.5] (see also [14, 15]) to give a full characterization of the algebraic closure of $\mathbb{F}_p(t)$ by generalizing the notion of automatic subsets of natural numbers to automatic subsets of S_p, where S_p is the set of nonnegative elements of $\mathbb{Z}[p^{-1}]$. As part of his work, he also shows that for these maps that arise, the "post-radix point behaviour" of such sets can be described in terms of sparse automatic sets.

Moosa and Scanlon's [35] (see also [24]) work on the isotrivial case of the Mordell-Lang conjecture deals with F-sets and these can again be described using sparse automatic sets (see, also, [12]). Finally, recent work by Bell, Hare and Shallit [11] shows that automatic sets that fail to be additive bases of the natural numbers can be characterized in terms of this sparse property as well.

While sparse automatic sets have played a fundamental role in many different areas of mathematics, thus far there has not been a systematic study of them from an algebraic/number theoretic point of view. In this thesis, we give a cohesive treatment of the theory of sparse automatic sets in three different contexts: the theory of algebraic power series, unlikely intersections, and the theory of representations in additive bases. In particular, we prove three different results on the theme of sparse automatic sets, the last of which is part of joint work with Jason Bell.

Our first result deals with a strong version of an old result of Cobham [16]. This result shows that if k and ℓ are two multiplicatively independent natural numbers ≥ 2 (i.e., there are no solutions to the equation $k^a = \ell^b$ with positive integers a and b), then if a set S is both k- and ℓ-automatic then in fact it is eventually periodic; that is, there is some fixed number c such that for n large, $n \in S \implies n + c \in S$. One can recast this as saying that if S is a k-automatic set and T is an ℓ-automatic set with k and ℓ again multiplicatively independent, then $S \cap T$ is a proper subset of S and T unless S and T are the same eventually periodic sets. Note that if S is a proper subset of T and T is eventually periodic, then $S \cap T$ is a proper subset of T but not of S. Since sparse non-empty sets cannot be eventually periodic, it is natural to consider whether a stronger version of this phenomenon might hold in the case of sparse sets (see Definition 24 in Section 2.2 for the definition of sparse sets). We show that this is indeed the case. Our first main result is the following theorem.

Theorem 1. *Let k and ℓ be multiplicatively independent natural numbers greater than or equal to 2. If S is a sparse k-automatic set and T is a sparse ℓ-automatic set then $S \cap T$ is finite.*

We prove this Theorem 1 in Chapter 4 by proving a stronger quantitative result that gives a bound on the size of the intersection in terms of the complexity of the machines needed to generate the sets S and T. To prove Theorem 1 we require the theory of S-units, and we shall give background on this in Chapter 3.

After this, we turn our attention to automatic sets that are additive bases of the natural numbers. Given a set S of natural numbers, we say that S is an *additive basis* of $\mathbb{N}$ of order d if every natural number can be expressed as the sum of d elements of S and no number smaller than d has this property. For example, a famous result of Lagrange says that the perfect squares $\{1, 4, 9, \ldots\}$ are an additive basis of the natural numbers of order four. (Note that seven cannot be written as a sum of three squares, so 4 is indeed the order of this additive basis.) A set is an additive basis if it is an additive basis of order d for some $d \geq 1$. Automatic sets that are additive bases of the natural numbers were characterized by Bell, Hare, and Shallit [11]. Interestingly, they showed that being an additive basis is equivalent to two conditions holding, one of which is that the set not be sparse and the other is that 1 must be in S.

This characterization allows one to examine classical questions about additive bases within the context of automatic sets. In particular, an old conjecture of Erdős and Turán [19] asserts the following: *if S is an additive basis of the natural numbers of order d then there are natural numbers n with arbitrarily many different representations as a sum of d elements of S*. There has been a lot of work on this question, but it nevertheless remains open today. We are able to show that their question has an affirmative answer for automatic sets.

Theorem 2. *Let k and d be positive integers greater than or equal to two and let S be a k-automatic set of natural numbers. If S is an additive basis of the natural numbers of order d then for each integer M there exists a natural number n such that the number of solutions to the equation $s_1 + \cdots + s_d = n$ with $(s_1, \ldots, s_d) \in S^d$ is at least M.*

Again we prove a quantitative version of this result in Chapter 5, showing that one can in fact find such an n that is bounded by a power function of N.

The final result of the thesis deals with refining the earlier-mentioned work of Christol, which characterized algebraic power series in terms of automatic sets. Christol showed that if q is a power of a prime p, then if $F(t) = \sum_{n \geq 0} f(n)t^n \in \mathbb{F}_q[[t]]$ is a power series that satisfies a non-trivial polynomial equation

$$P(t, F(t)) = 0$$

with $P(X, Y) \in \mathbb{F}_q[X, Y]$, then for each $a \in \mathbb{F}_q$ the set of n for which $f(n) = a$ is a p-automatic subset of $\mathbb{N}$. In particular, the *support* of $F(t)$ (the set of n for which $f(n) \neq 0$) is p-automatic, since finite unions of p-automatic sets are again p-automatic.

With the sparse/non-sparse dichotomy for automatic sets mentioned above, a natural question to ask is whether one can give a characterization of the algebraic power series over a finite field with sparse supports. The author, in joint work with her supervisor [1], gives such a characterization from two different points of view.

In this work it is shown that such series with sparse supports are intimately linked with Artin-Schreier extensions, whose existence is the main reason for the fact that the algebraic closure of the field of Laurent series $K((t))$ over a field K is considerably simpler when K is of characteristic zero than when it is of positive characteristic.

We show that the collection of algebraic power series with sparse supports (henceforth called *sparse series*) forms a ring and characterize this ring in two ways. The first characterization is that the collection of sparse series is the smallest non-trivial subalgebra closed under certain sparseness-preserving operators, such as making a change of variables by multiplying the variable by a nonzero scalar, substituting a power of the variable as the new variable, or multiplying (or dividing) the series by a power of the variable, along with a special operator related to the Frobenius map. Our second characterization is purely algebraic and is given by taking the integral elements in a certain maximal unramified extension. Background on ramification and necessary algebraic concepts is provided in Chapter 3. More specifically, the final result of this thesis is the following and is proved in Chapter 6.

Theorem 3. *Let p be a prime and let A be the field extension of $\bar{\mathbb{F}}_p(t)$ consisting of algebraic Laurent series over $\bar{\mathbb{F}}_p$, and let B be the subring of A consisting of algebraic power series with sparse support. Then we have the following:*

(a) B is the smallest non-trivial $\bar{\mathbb{F}}_p$-subalgebra of A that possesses the following closure properties:

(P1) If $F(t) \in B$ and $F(0) = 0$ then $F(t) + F(t^p) + F(t^{p^2}) + \cdots \in B$;

(P2) If $F(t) \in B$ and $\alpha \in \bar{\mathbb{F}}_p$ then $F(\alpha t) \in B$;

(P3) if $F(t) \in B$ and $t^d F(t^c) \in A$ with $c \in \mathbb{Q}_{>0}$ and $d \in \mathbb{Q}$, then $t^d F(t^c) \in B$;

(b) If $F(t)$ is a power series with coefficients in $\bar{\mathbb{F}}_p$ then $F(t) \in B$ if and only if there is some $j \geq 0$ such that for $G(t) := F(t^{p^j})$ the following hold:

(i) the Galois closure of $G(t)$ over the field $K := \bar{\mathbb{F}}_p(t^{\pm 1/n} : n \geq 1, p \nmid n)$ has degree a power of p;

(ii) the extension $K(G(t))/K$ is unramified outside of 0 and ∞;

(iii) $G(t)$ *is integral over the Laurent polynomial ring* $\bar{\mathbb{F}}_p[t^{\pm 1}]$.

We point out that the technical terminology used in the statement of Theorem 3 is defined in Chapter 3. We also point out that in item (ii) in part (b) of the statement of Theorem 3, we are implicitly using the fact that places of K are parameterized by points in $\mathbb{P}^1_{\bar{\mathbb{F}}_p}$ (see Chapter 6 for details) and so it is this identification of places with points in projective space that is being used when we speak of unramified extensions outside of 0 and ∞.

The outline of the thesis is as follows. In Chapters 2 and 3, the necessary background on the theory of automatic sets and sequences and on number theory is given. In Chapter 4 we prove a quantitative version of Theorem 1 and in Chapter 5 we prove a quantitative version of Theorem 2. In Chapter 6, Theorem 3 is proved along with a more general result characterizing generalized Laurent series with sparse support, which arise in Kedlaya's extension of Christol's theorem. Finally, in Chapter 7, we briefly consider the possibility of finding the right extension of sparseness to regular sequences.

Chapter 2

Preliminaries on Automata

In this chapter, we give some of the basic background on automata required to understand the main results of this thesis. We introduce deterministic finite automata with output, k-automatic sequences, and examine various equivalent definitions of these concepts. We also introduce k-automatic sets and look at some examples. Then we define sparse languages and look at some properties of sparse automatic sets. We present Christol's theorem, which provides a bridge between p-automatic sequences and formal power series that are algebraic. Then we present generalized series, which are used by Kedlaya to extend Christol's Theorem, together with the corresponding generalization of p-automatic sets. Kedlaya's theorem characterizes the full algebraic closure of function fields in terms of p-quasi-automatic sets. Much of the exposition in this chapter follows material from [2, 8, 28, 29, 31].

2.1 Automatic Sequences and Sets

In this section, we give some elementary information concerning regular languages, finite-state automata, and p-automatic sequences. We start by setting the stage as follows. Let Σ be a nonempty finite set. We call Σ an *alphabet* and we call a finite or infinite sequence of symbols chosen from Σ a *word* over the alphabet Σ. Given a finite-length word $w = a_r a_{r-1} \dots a_1 a_0$, we define its reversal $w^R = a_0 a_1 \dots a_{r-1} a_r$. We let Σ^* denote the set of all finite words over Σ; that is, Σ^* is the free monoid on the set Σ, with multiplication given by concatenation. A language over Σ is a subset of Σ^*. We say that a language $\mathcal{L} \subseteq \Sigma^*$ is a *regular language* if there is a finite-state machine accepting $\mathcal{L}$ (see Kleene's theorem [30]). Having given some terminology, we now see how this works in practice.

Finite-state machines take words over a finite alphabet as input. They read the word by starting from an initial state and moving from state to state as each letter is read. After the reading of the word is done, according to which state is reached at the end, the machine decides to accept the word or not to accept it.

As an example we look at Figure 2.1, which depicts a deterministic finite-state machine which accepts all the words over the alphabet $\Sigma_2 = \{0, 1\}$ which contain two consecutive 1's and rejects all the others. The states at which a word ends up and are accepted are indicated with double-circles. The rest of the states (at which a word ends up and are rejected) are indicated with single-circles. The state at which the machine starts reading a word is labeled q_0 and the rest of the states are labeled accordingly. To indicate how the machine works, we include paths (or arrows) with labels to indicate which state is reached after which letter is read. For example in Figure 2.1, when a word starts being read, the machine starts at q_0 and if it reads a 0 it remains at the same state q_0, if it reads a 1 it moves to state q_1. More concretely, when $w = 01101$ is being read (from right to left), we start at q_0, reading 1 we move to q_1, we then read 0 and move back to q_0, read 1 and move to q_1, read one more 1 and move to q_2; reading 0 while we are at q_2, we stay at q_2, as indicated by the labeled arrows. After the reading is done, the state reached is q_2 and it is double circled. So this machine accepts the word 01101. This is no coincidence because we constructed this machine so that it accepts words that contain two consecutive 1's. Next consider the example 010101. Then reading from right to left we go from q_0 to q_1, q_0, q_1, q_0, q_1, q_0, respectively. Since the state reached after the word is read is q_0 and since q_0 is not one of the accepting (double-circled) states, we conclude that the word 010101 is rejected by this machine.

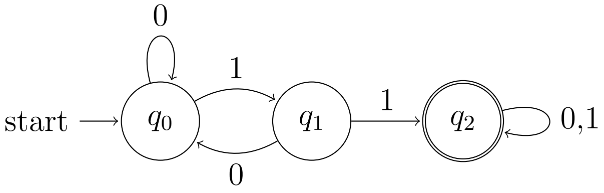

Figure 2.1: A deterministic finite-state machine (or a deterministic finite automaton)

Observe that at each state the various letters of our input alphabet give transitions to other states and we can think of this as giving a function from the Cartesian product of the set of states and the input alphabet to the set of states. For the finite-state machine in Figure 2.1, call the collection of all states Q and we can define $\delta : \Sigma_2 \times Q \to Q$ by $\delta(0, q_0) = q_0$, $\delta(1, q_0) = q_1$, $\delta(0, q_1) = q_0$, $\delta(1, q_1) = q_1$, $\delta(0, q_2) = q_2$, and $\delta(1, q_2) = q_2$. In addition to these data, we also require a set of accepting states $A \subseteq Q$. Then for the finite automaton given in Figure 2.1, $A = \{q_2\}$. More formally, we give the definition of a deterministic finite-state automaton below.

Definition 4. A *deterministic finite-state machine* or a *deterministic finite automaton* (DFA) is a 5-tuple $(Q, \Sigma, \delta, q_0, A)$ where Q is a finite set of states, Σ is a finite input alphabet, δ is a transition function from $\Sigma \times Q$ to Q, $q_0 \in \Sigma$ is an initial state, and $A \subseteq Q$ is a set of accepting states.

If we consider accepting a word as giving an output of 1 and rejecting as giving 0, we can add one more function to this 5-tuple and make it a deterministic finite-state machine with output. In this case the output function is defined from the set of all states to the set $\{0, 1\}$. For example, for the DFA in Figure 2.1, the output function $\tau : Q \to \{0, 1\}$ can be defined by setting $\tau(q_0) = \tau(q_1) = 0$, $\tau(q_2) = 1$. Notice that the data of this function now adds an output alphabet to the 5-tuple and also makes indicating the set of accepting states redundant because they are now characterized by the function τ. In this case Figure 2.1 becomes Figure 2.2, where we remove the double-circles and instead label the state q_i along with its output as $q_i/\tau(q_i)$. Extending this idea, one can have any alphabet as the range of the output function τ.

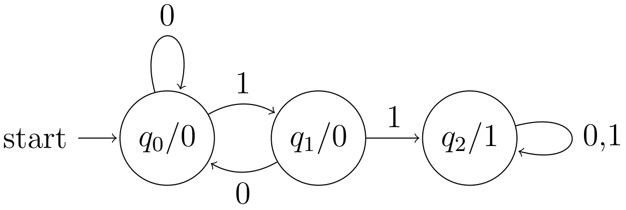

Figure 2.2: A deterministic finite automaton with output (DFAO)

We now give a formal definition of the idea behind the above-described machine.

Definition 5. A *deterministic finite automaton with output* (DFAO) is a 6-tuple

$$M = (Q, \Sigma, \delta, q_0, \Delta, \tau),$$

where Q is a finite set of states, Σ is a finite input alphabet, δ is the transition function from $\Sigma \times Q$ to Q, $q_0 \in Q$ is the initial state, Δ is an output alphabet, and τ is the output function from Q to Δ.

Intuitively, we can think of a DFAO as a directed graph in which the vertices are the elements of Q and for each vertex $q \in Q$ and each $s \in \Sigma$ we have a directed arrow with label s from q to the state $q' = \delta(s, q)$. Then given a word $w \in \Sigma^*$, the DFAO gives us an output in Δ as follows: we begin at the initial state q_0 and then, reading w from right to left, we obtain a path by moving vertex to vertex as we read each letter in w. When we have finished reading w, we arrive at a state $q \in Q$ and we then apply τ to obtain an output in Δ. Adopting this point of view, we see we can extend δ to a map from $\Sigma^* \times Q$ to Q and then the output associated with a word $w \in \Sigma^*$ is simply $\tau(\delta(w, q_0))$. Thus to a DFAO M, there is an associated finite-state function $f_M : \Sigma^* \to \Delta$ given by $f_M(w) = \tau(\delta(w, q_0))$.

For a natural number $k \geq 2$, we let

$$\Sigma_k = \{0, 1, \ldots, k-1\}, \tag{2.1}$$

which are the digits used in forming base-k expansions of natural numbers. For every natural number n, there is a word $w = (n)_k \in \Sigma_k^*$, which is the base-k expansion of n, where we define $(0)_k$ to be the empty word; conversely, given a non-empty word $w \in \Sigma_k^*$ with no leading zeros there is a natural number $n = [w]_k$, which is the natural number whose base-k expansion is w. In the case when w is the empty word, we take $[w]_k = 0$. If $w = a_1 a_2 \cdots a_{s-1}$, we have

$$[w]_k = \sum_{i=1}^{s-1} a_i k^{s-1-i},$$

and if

$$n = \sum_{i=1}^{s-1} a_i k^{s-1-i}$$

with a_1 nonzero then $(n)_k = a_1 a_2 \cdots a_{s-1}$.

If we use the base-k expansions of the natural numbers as the input for a DFAO $M = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$, then for each natural number n, we get an output computed by M; i.e., M generates a sequence $f(n)$ taking values in Δ, where we set $f(n) = f_M((n)_k)$ with $n = [w]_k$ and $f_M(w) = \tau(\delta(w, q_0))$. Such a DFAO is called a *k-DFAO*.

Let us look at a concrete example (see Figure 2.3) of a k-DFAO which generates a famous sequence, the Thue-Morse sequence. This is a 2-DFAO, hence having input alphabet $\Sigma_2 = \{0, 1\}$, and it has two states q_0 and q_1, with q_0 being the initial state. Its transition function is given by $\delta(0, q_0) = q_0$, $\delta(0, q_1) = q_1$, $\delta(1, q_0) = q_1$, and $\delta(1, q_1) = q_0$. The labelling $q_0/0$ and $q_1/1$ inside states is specifying that $\tau(q_0) = 0$ and $\tau(q_1) = 1$. If we regard a word over the alphabet Σ_2 with no leading zeros as being the binary expansion of a natural number then we can construct a $\{0, 1\}$-valued sequence $f(n)$ by feeding the binary expansion of n into our DFAO, starting at state q_0 and reading the word from right to left, and then (to get the value) applying τ to the state we reach after we have fed all of the digits into the machine. For example, if $n = 13$, we have the binary expansion 1101, and applying successive transitions we see that 1101 takes state q_0 to state q_1 and so $f(13) = \tau(q_1) = 1$. The sequence obtained in this particular case via this procedure is known as the Thue-Morse sequence.

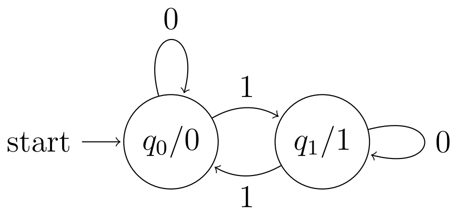

Figure 2.3: A 2-DFAO generating the Thue-Morse sequence.

We record the type of sequences generated in this way in the following definition.

Definition 6. Let Δ be a finite set. A function $a : \mathbb{N} \to \Delta$ is called a *k-automatic sequence* if there exists a k-DFAO M with output alphabet Δ such that for each $n \in \mathbb{N}$, $a(n)$ is equal to $f_M\left((n)_k\right)$.

For example, the Thue-Morse sequence is a 2-automatic sequence and it is generated by the 2-DFAO drawn in Figure 2.3. One can also explicitly write a formula for the terms of the Thue-Morse sequence. Let $\{t(n)\}_{n=0}^{\infty}$ denote the Thue-Morse sequence. Define $s(n)$ to be equal to the number of 1's in the base-2 expansion of n. Then $t(n)$ can be defined for each n as follows:

$$t(n) = \begin{cases} 0 & \text{if } s(n) \equiv 0 \pmod 2 \\ 1 & \text{if } s(n) \equiv 1 \pmod 2. \end{cases} \tag{2.2}$$

With this definition, one can write down the first few terms of the Thue-Morse sequence:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
$t(n)$	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	...

Note that it is also possible to define this sequence by the recursive formulas

$$\begin{aligned} t(0) &= 0, \\ t(2n) &= t(n), \\ t(2n+1) &= 1 - t(n). \end{aligned} \tag{2.3}$$

Another basic example of a k-automatic sequence is, for a fixed prime number p,

$$a(n) = \begin{cases} 1 & \text{if } n = p^m \text{ for some integer } m \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{2.4}$$

Then we can show that there exists a p-DFAO M (with finite-state function f_M) such that $a(n)$ can be computed as $f_M((n)_k)$. In the case when $p = 2$, the automaton accepting the base-p expansions of powers of p is given in Figure 2.4. Notice that the sequence $a(n)$ coincides with the characteristic function of the set of powers of p, which we will elaborate on later, when we define k-automatic sets.

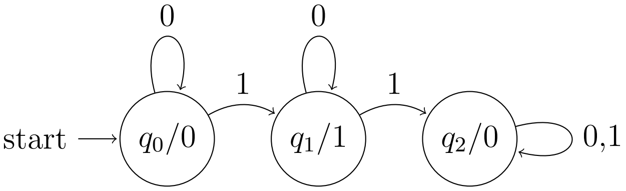

Figure 2.4: A deterministic finite-state machine accepting the binary expansions of powers of 2.

There are many equivalent characterizations of k-automatic sequences, one of which is done using the notion of k-kernels and another is given by using morphisms (Cobham's little theorem). Before we jump to these equivalent definitions, let us prove a basic property of automatic sequences using the definition we have seen so far.

Notation 7. *For a sequence $\{a(n)\}_{n=0}^{\infty}$, we write $\{a(n)\}_n$ for simplicity.*

Lemma 8. *Let $\{a(n)\}_n$ and $\{b(n)\}_n$ be k-automatic sequences with values in alphabets Δ and Δ'. Then the sequence $\{c(n)\}_n$ defined by $c(n) := (a(n), b(n))$ for each $n \geq 0$ is also k-automatic.*

Proof. Since $\{a(n)\}_n$ and $\{b(n)\}_n$ are k-automatic sequences, there exist k-DFAOs M and M' with $M = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$ and $M' = (Q', \Sigma_k, \delta', q_0', \Delta', \tau')$ that generate the sequences $\{a(n)\}$ and $\{b(n)\}$, respectively. Using M and M', we construct a new k-DFAO that will generate the sequence $\{c(n)\}_n$. Let

$$M'' = (Q \times Q', \Sigma_k, \delta'', (q_0, q_0'), \Delta \times \Delta', \tau''),$$

where we define δ'' and τ'' for each $q \in Q, q' \in Q', n \in \Sigma$ as follows: $\delta''((q, q'), (n)_k) = (\delta(q, (n)_k), \delta'(q', (n)_k))$ and $\tau''(q, q') = (\tau(q), \tau'(q'))$. Then this new k-DFAO generates the sequence $\{c(n)\}_n$. To see this, we prove $c(n) = \tau''(\delta''((q_0, q_0'), (n)_k))$. We have $\delta''((q_0, q_0'), (n)_k)) = (\delta(q_0, (n)_k), \delta'(q_0', (n)_k))$ by definition of δ''. Then $\tau''(\delta''((q_0, q_0'), (n)_k)) = \tau''(\delta(q_0, (n)_k), \delta'(q_0', (n)_k)) = (\tau(\delta(q_0, (n)_k)), \tau'(\delta'(q_0', (n)_k))) = (a(n), b(n)) = c(n)$. □

We now look at an equivalent definition of k-automatic sequences in terms of k-kernels.

Definition 9. For $k \geq 2$ and a sequence $\{u(n)\}_n$, the *k-kernel* of $\{u(n)\}_n$ is defined as

$$K_k = \left\{ \{u(k^i n + j)\}_n : i \geq 0 \text{ and } 0 \leq j < k^i \right\}.$$

Most sequences have infinitely many distinct subsequences that occur in the k-kernel, but for k-automatic sequences the kernel is finite and this in fact characterizes the property of k-automaticity. An example is the Thue-Morse sequence. It has 2-kernel $K = \{\{t(2n)\}_n, \{t(2n+1)\}_n\}$ by the relations in Equation 2.3. So $\{t(n)\}_n$ has finite 2-kernel (with 2 elements). This shows that the Thue-Morse sequence is 2-automatic without having to explicitly write a finite-state machine that generates it, by the well-known characterization below (see Allouche and Shallit [2, Theorem 6.6.2]).

Theorem 10. *Let $k \geq 2$. A sequence is k-automatic if and only if its k-kernel is finite.*

This characterization of automaticity is useful when exploring some properties of k-automatic sequences. We now give another characterization of automaticity due to Cobham [17]. This characterization of k-automatic sequences involves morphisms and can be used to prove additional properties of k-automatic sequences. For example, Proposition 18, which states a sequence is k-automatic if and only if it is k^m-automatic can be quickly proved using Cobham's characterization. This property will later be useful in proving Christol's theorem relating algebraic power series to automata. To provide necessary background for Cobham's little theorem, we briefly review morphisms and uniform morphisms along with giving some examples.

Definition 11. Let Σ and Δ be alphabets. A *morphism* is a map f from Σ^* to Δ^* satisfying $f(ab) = f(a)f(b)$ for all $a, b \in \Sigma^*$.

Note that when specifying a morphism, it is sufficient to define f on the elements of Σ since we can then extend it uniquely to a morphism from Σ^* to Δ^*. Note also that the identity $h(xy) = h(x)h(y)$ for all $x, y \in \Sigma^*$ forces $h(\epsilon) = \epsilon$, where ϵ is the empty word.

Example 12. Let $\Sigma = \{t, h, e, s, i\}$ and $\Delta = \{d, i, s, e, r, t, a, o, n\}$. Set $f(t) = di$, $f(h) = ss$, $f(e) = er$, $f(s) = \epsilon$ and $f(i) = tation$. Then $f(thesis) = dissertation$.

Definition 13. Let $k \geq 2$ be a positive integer and let Σ and Δ be finite alphabets. A *k-uniform morphism* $f : \Sigma^* \to \Delta^*$ is a morphism such that $|f(a)|$, the length of the word $f(a)$, is equal to k for all $a \in \Sigma$. A 1-uniform morphism is called a *coding*.

We have seen the Thue-Morse sequence is generated by a 2-DFAO and that it has a finite 2-kernel. Now we also show that it is the image of a 2-uniform morphism, which will constitute another method of proving the Thue-Morse sequence is 2-automatic, by using Cobham's little theorem (see Theorem 17 below).

It is noteworthy to mention that the image of an automatic sequence under a coding is also automatic. We record this more formally.

Lemma 14. *If $a : \mathbb{N} \to \Delta$ is a k-automatic sequence for some finite set of symbols Δ and if f is a function from Δ to a set Z, then $\{f(a(n))\}_n$ is also a k-automatic sequence taking values in a finite subset of Z.*

Proof. Since the sequence $\{a(n)\}_n$ is k-automatic, there exists a k-DFAO that generates it. Denote it by $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$. Then for each $n \geq 0$, we have $a(n) = \tau(\delta(q_0, (n)_k))$. Now we can make a new k-DFAO by replacing the map τ by $f \circ \tau$, and the output alphabet Δ by $f(\Delta)$. Hence the k-DFAO $(Q, \Sigma, \delta, q_0, f(\Delta), f \circ \tau)$ generates $\{f(a(n))\}_n$. □

Combining Lemmas 8 and 14, we get the following corollary.

Corollary 15. *Let $\{a(n)\}_n$ and $\{b(n)\}_n$ be two k-automatic sequences taking values in a finite subset of a ring R. Then:*

(i) $\{a(n) + b(n)\}_n$ *is k-automatic,*

(ii) $\{a(n)b(n)\}_n$ *is k-automatic,*

(iii) $\{c\, b(n)\}_n$ *is k-automatic for any constant $c \in \mathbb{Z}$.*

Proof. Let $c(n) = (a(n), b(n))$. Then by Lemma 8, $c(n)$ is k-automatic. Let R_a and R_b be two finite subsets of R such that $a(n) \in R_a$ for all $n \geq 0$ and $b(n) \in R_b$ for all $n \geq 0$. Then $c(n)$ takes finitely many values, namely it has values in $R_a \times R_b$. Now we will use different maps $f : R_a \times R_b \to R$, using that the image of an automatic sequence under a coding is again automatic, to obtain the three parts:

(i) by taking $f(x, y) := x + y$.

(ii) by taking $f(x, y) := xy$.

(iii) by taking $a(n)$ to be the constant sequence c with $c \in \mathbb{Z}$ and applying part (ii). Every constant sequence is k-automatic since it has one element in its k-kernel.

□

Next we give a calculation that shows how to compute the image of a letter in an infinite word under a uniform morphism. This will be useful in proving Cobham's little theorem (Theorem 17). We follow the treatment of this result in the text of Allouche and Shallit [2, Chapter 6].

Lemma 16. *Let $k \geq 2$ and suppose that f is a k-uniform morphism. If $w = a_0 a_1 a_2 \ldots$ is a fixed point of f, then $f(a_i) = a_{ki} \ldots a_{ki+k-1}$.*

Proof. Since w is a fixed point of f and f is a k-uniform morphism, $f(a_0 \cdots a_i) = a_0 \cdots a_{ki+k-1}$. We can write

$$\begin{aligned} f(a_0 \cdots a_i) &= f(a_0 \cdots a_{i-1}) f(a_i) \\ &= a_0 \cdots (a_{k(i-1)+k-1}) a_{ki} \ldots a_{ki+k-1}, \end{aligned}$$

which proves that $f(a_i) = a_{ki} \ldots a_{ki+k-1}$. □

The following theorem goes by the name Cobham's little theorem [17].

Theorem 17. *Let $k \geq 2$. Then a sequence $\{a(n)\}_n$ is k-automatic if and only if it is the image, under a coding, of a fixed point of a k-uniform morphism.*

Proof. This argument is simpler if one works with automata that read base-k expansions from left-to-right. Fortunately, this is equivalent to the right-to-left definition we have worked to up till now (cf. Allouche and Shallit [2, Corollary 4.3.5]). We will add the adjective *left-to-right* when describing k-DFAOs with the property of reading words starting from the left.

Suppose that $\{a(n)\}_n$ is k-automatic. Then there exists a left-to-right k-DFAO $(Q, \Sigma_k, \delta, q, \Delta, \tau)$ that generates it. We may assume $\delta(q_0, 0) = q_0$ by adding a new initial state to the k-DFAO and redefining the maps δ and τ, if necessary. Now we define a morphism $f : Q^* \to Q^*$ as follows. For $q \in Q$, we let $f(q) = \delta(q, 0) \cdots \delta(q, k-2)\delta(q, k-1) \in \Delta^*$. Let $w = w_0 w_1 w_2 \cdots$ be the unique fixed point of f with $w_0 = q_0$. (This is obtained by taking the limit of $f^n(q_0)$ where f^n is the n-th iterate of f.) We can show $\delta(q_0, y) = w_{[y]_k}$ for all $y \in \Sigma^*$ by induction on the length of y. If the length of y is zero, then $\delta(q_0, 0) = q_0 = w_0$. Assume $\delta(q_0, y) = w_{[y]_k}$ for all $y \in \Sigma^*$ with $|y| < i$. Let $|y| = i$. Writing $y = xa$, where $a \in \Sigma_k$ and $|x| = i - 1$, we have

$$\begin{aligned}\delta(q_0, y) &= \delta(q_0, xa)\\ &= \delta(\delta(q_0, x), a)\\ &= \delta(w_{[x]_k}, a), \text{ by the induction hypothesis}\\ &= a\text{th letter in } f(w_{[x]_k}), \text{ by definition of } f\\ &= w_{k[x]_k+a}, \text{ by Lemma 16}\\ &= w_{[xa]_k}\\ &= w_{[y]_k}.\end{aligned}$$

So, we get $a(n) = \tau(\delta(q_0, (n)_k)) = \tau(w_n)$. Hence $\{a(n)\}_n$ is the image (under τ) of a fixed point of f.

For the other direction, let Q and Δ be finite alphabets, let $\tau : Q \to \Delta$ be a coding, and suppose $\{a(n)\}_n$ is the image of τ applied to the fixed point, w, of a k-uniform morphism $\phi : Q^* \to Q^*$. Let w_i denote the i-th letter of the word w for $i \geq 0$. Define a (left-to-right) k-DFAO $M = (Q, \Sigma_k, \delta, w_0, \Delta, \tau)$ where $\delta(q, b)$ is the b-th letter of $\phi(q)$. We claim that $w_n = \delta(w_0, (n)_k)$ for all $n \geq 0$. We prove it by (strong) induction on n. For $n = 0$, we have $\delta(w_0, 0) = w_0$. Now suppose that $w_i = \delta(w_0, (i)_k)$ for all $i < n$. Let $(n)_k = n_t n_2 \ldots n_1$, so $n = kn' + n_1$, for some n' and $0 \leq n_1 < k$. Then we have

$$\begin{aligned}\delta(w_0, (n)_k) &= \delta(w_0, n_t n_{t-1} \ldots n_2 n_1)\\ &= \delta(\delta(w_0, n_t \ldots n_2), n_1)\\ &= \delta(\delta(w_0, (n')_k, n_1)\\ &= \delta(w_{n'}, n_1)\\ &= n_1\text{-th letter of } \phi(w_{n'})\\ &= w_{kn'+n_1}, \text{ by Lemma 16}\\ &= w_n.\end{aligned}$$

Then $a(n) = \tau(w_n) = \tau(\delta(q_0, (n)_k)$. □

This theorem helps us understand how outputs of two automata with different alphabets relate to each other in a special case, namely, when one alphabet has cardinality a power of the cardinality of the other automaton's alphabet.

Proposition 18. *Let $k \geq 2$ and $m \geq 1$ be natural numbers. A sequence $\{a(n)\}_n$ is k-automatic if and only if it is k^m-automatic.*

Proof. By Cobham's little theorem (Theorem 17), if $\{a(n)\}_n$ is k-automatic, then it can be expressed as the image under a coding τ of a fixed point of a k-uniform morphism f. So, we have

$$a_0a_1a_2 \cdots = \tau(f^\omega(a_0)) \text{ for some letter } a_0,$$

where $f(a_0)$ has a_0 as a prefix and $f^\omega(a_0)$ represents the infinite word obtained by taking the limit of $f^n(a_0)$ as n tends to infinity. If $g := f^m$, then g is a k^m-uniform morphism and we have $a_0a_1a_2 \cdots = \tau(g^\omega(a_0))$. So, $\{a(n)\}_n$ is k^m-automatic by Cobham's little theorem.

If $\{a(n)\}_n$ is k^m-automatic, then its k^m-kernel is finite. Denote its k^m-kernel by

$$K' = \{\{a(k^{mi}n + b)\}_n : i \geq 0, 0 \leq b < k^{mi}\} := \{\{a_1(n)\}_n, \ldots, \{a_d(n)\}_n\}$$

for some finite set of sequences $a_1, \ldots, a_d$. We want to show that the k-kernel $K_k = \{\{a(k^sn + t)\}_n : s \geq 0, 0 \leq t < k^s\}$ is finite. Given $s \geq 0$ and t with $0 \leq t < k^s$, we can write $s = mq + r$ where $0 \leq r < m$ and $t = k^{mq}t_1 + t_0$ where $t_0 < k^{mq}$. Notice that $t_1 < k^r$ since $t < k^s$. Then we have

$$k^sn + t = k^{qm+r}n + k^{qm}t_1 + t_0 = k^{qm}(k^r + t_1) + t_0.$$

Then $a(k^sn + t) = a(k^{qm}(k^rn + t_1) + t_0)$ but $a(k^{qm}(k^rn + t_1) + t_0) = a_i(k^rn + t_1)$ for some i, by definition of K'. There are only finitely many sequences of the form $a_i(k^rn + t_1)$ since $i \leq d$, $r < m$ and $t_1 < k^r$. Hence we are done. □

We revisit the sequence generated by the finite-state machine in Figure 2.4. The values of the sequence are obtained by looking the characteristic function of the set $S = \{1, p, p^2, p^3, p^4, \ldots\}$ consisting of powers of p, for a prime number p; i.e.,

$$\chi_S(n) = \begin{cases} 1 & \text{if } n \in S \\ 0 & \text{if } n \notin S. \end{cases}$$

Definition 19. Let $k \geq 2$ be a positive integer and let S be a subset of nonnegative integers. Then S is called *k-automatic* if $\{\chi_S(n)\}_n$ is a k-automatic sequence.

In the above example, the sequence $(\chi_S(n))_{n\geq 0}$ is a p-automatic sequence, where $S = \{1, p, p^2, p^3, p^4, \ldots\}$, and so S is a p-automatic set.

We can prove certain closure properties of k-automatic sets by using Definition 19.

Proposition 20. *Let $k \geq 2$ and let S and T be k-automatic subsets of $\mathbb{N}$. Then*

(i) $S \cup T$ is k-automatic, and

(ii) $S \cap T$ is k-automatic.

Proof. We consider the characteristic functions of the sets $S \cup T$ and $S \cap T$. Then we have

$$\chi_{S\cup T}(n) = \chi_S(n) + \chi_T(n) - \chi_S(n)\chi_T(n)$$

and

$$\chi_{S\cap T}(n) = \chi_S(n)\chi_T(n).$$

The automaticity of $S \cup T$ and $S \cap T$ now follows from parts (i) and (ii) of Corollary 15. □

In the next section, we turn our attention to the main focus of this thesis: sparse automatic sets, which form a distinguished subclass of the class of automatic sets.

2.2 Sparse Automatic Sets

In this section we give an overview of sparse languages and sparse sets. We revisit some well-known material from [12] (for example, Proposition 22). We let Σ be a finite alphabet and we let $\mathcal{L} \subseteq \Sigma^*$ be a language. We define the counting function of the language

$$f_{\mathcal{L}}(n) := \#\{w \in \mathcal{L} \colon \text{length}(w) \leq n\}.$$

A regular language is sparse if the number of words of length at most n grows at most polynomially in n. More precisely, we shall say that a regular language $\mathcal{L}$ is *sparse* if one of the equivalent conditions in Proposition 22 below holds. Sparse languages play an integral role in the theory of regular languages and finite-state automata, and they have been studied in numerous contexts. We borrow a summary of conditions equivalent to sparseness from [12], which combines results from [23, 25, 27, 43, 44].

We introduce some notation that will be used here and in later sections.

Notation 21. *Let $f(x)$ and $g(x)$ be two real-valued functions with g strictly positive. We write $f(x) = \mathrm{O}(g(x))$ for all sufficiently large x if there exists a positive constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for sufficiently large x. We write $f(x) = \mathrm{o}(g(x))$ for all sufficiently large x if for every $\epsilon > 0$ there exists a constant $N \geq 1$ such that $|f(x)| \leq \epsilon|g(x)|$ for all $x \geq N$.*

Proposition 22. *Let $\mathcal{L}$ be a regular language. Then the following are equivalent:*

(1) $f_{\mathcal{L}}(n) = \mathrm{O}(n^d)$ *for some natural number* d.

(2) $f_{\mathcal{L}}(n) = \mathrm{o}(C^n)$ *for every* $C > 1$.

(3) There do not exist words u, v, a, b *with* a, b *non-trivial and of the same length and* $a \neq b$ *such that* $u\{a, b\}^* v \subseteq \mathcal{L}$.

(4) Suppose $\Gamma = (Q, \Sigma, \delta, q_0, F)$ *is an automaton accepting* $\mathcal{L}$ *in which all states are accessible. Then* Γ *satisfies the following.*

  (*) If q *is a state such that* $\delta(q, v) \in F$ *for some word* v *then there is at most one non-trivial word* w *with the property that* $\delta(q, w) = q$ *and* $\delta(q, w') \neq q$ *for every non-trivial proper prefix* w' *of* w*;*

(5) There exists an automaton accepting $\mathcal{L}$ *that satisfies* $(*)$.

(6) $\mathcal{L}$ *is a finite union of languages of the form* $v_1 w_1^* v_2 w_2^* \cdots v_k w_k^* v_{k+1}$ *where* $k \geq 0$ *and the* v_i *are possibly trivial words and the* w_i *are non-trivial words.*

Given the connection between regular languages over the alphabet $\{0, 1, \ldots, k-1\}$ and k-automatic sets, we can naturally extend the notion of sparseness to k-automatic sets as follows. Given a subset $S \subseteq \mathbb{N}$, we say that S is a *sparse* k-automatic set if $\{(n)_k \in \{0, 1, \ldots, k-1\}^* \colon n \in S\}$ is a sparse sublanguage of $\{0, 1, \ldots, k-1\}^*$. If one translates conditions (i) and (ii) of Proposition 22 into this context, we obtain the following dichotomy.

Theorem 23. *Let* $S \subseteq \mathbb{N}$ *be a* k*-automatic set and let* $\pi_S(x) := \#\{n \in S \colon n \leq x\}$ *for* $x \geq 0$. *Then one of the following alternatives must hold:*

(1) there exists $d \geq 1$ *such that* $\pi_S(n) = O((\log n)^d)$ *as* $n \to \infty$*; or*

(2) there exists a real number $\alpha > 0$ *such that* $\pi_S(n) > n^\alpha$ *for all sufficiently large* n.

Then sparse sets are precisely k-automatic sets for which there is some $d \geq 1$ such that $\pi_S(n) = O((\log n)^d)$, and this “gap” result shows there is a clear delineation between sparse and non-sparse k-automatic sets. We record this more formally.

Definition 24. Let $k \geq 2$ be a natural number and let S be a k-automatic set. We say that S is *sparse* if condition (1) in Theorem 23 holds.

One can in fact take the finite union given in item (6) of Proposition 22 to be disjoint. This fact is not explicitly stated in [12, Proposition 7.1], and so we provide an argument below.

Lemma 25. *Let $\mathcal{L}$ be a regular sparse language. Then, the language $\mathcal{L}$ is a finite disjoint union of languages of the form*

$$v_1 w_1^* v_2 w_2^* \cdots v_s w_s^* v_{s+1}$$

where $s \geq 0$, the v_i are possibly trivial words and the w_i are non-trivial words.

Proof. We will work with automata that read expansion from left-to-right since the argument is completely symmetric.

We know by Proposition 22 that the language $\mathcal{L}$ is a finite union of languages of the form

$$v_1 w_1^* v_2 w_2^* \cdots v_s w_k^* v_{s+1}$$

where $s \geq 0$ and the v_i are possibly trivial words and the w_i are non-trivial words. We only need to show that this finite union can be taken as a disjoint union of languages of this form. Let $\Gamma = (Q, \Sigma, \delta, q_0, F)$ be a finite-state automaton accepting $\mathcal{L}$. We recall that condition $(*)$ in item (4) of Proposition 22 also holds because $\mathcal{L}$ is a sparse language.

One can define an equivalence relation on the set of states as follows. Given two states q, q', we'll say that $q \prec q'$ if there is some $u \in \Sigma^*$ such that $\delta(q, u) = q'$. If $q \prec q'$ and $q' \prec q$, we'll write $q \sim q'$. We note that $\sim$ is an equivalence relation and $\prec$ induces a partial order on the equivalence classes and we'll let $[q]$ denote the equivalence class of q. Since $\mathcal{L}$ is sparse, there is a unique (possibly empty) cycle that visits each state in an equivalence class.

We now prove the decomposition for $\mathcal{L}$ by induction on the number of equivalence classes in Q. If there is a single equivalence class, then there is a unique cycle corresponding to the word w based at q_0 that visits each state in $[q_0]$. Then every word accepted by our language is of the form $w^n v$ where v is a prefix of w. Thus our language $\mathcal{L}$ is a finite disjoint union of languages of the form $w^* v$ in this case. Now we suppose that the claim holds whenever there are fewer than d equivalence classes in Q and we consider the case when there are d classes. Then there is a shortest word w (that is possibly empty) that visits each state in $[q_0]$ and a word in $\mathcal{L}$ either has $\delta(q_0, w) \in [q_0]$ or $\delta(q_0, w) \notin q_0$. In the former case, we get a finite disjoint set of languages of the form $w^* v$ with v a prefix of w and we call this union $\mathcal{L}_0$; in the latter case, we get a finite disjoint union of languages of the form $w^* u_i \mathcal{L}_i$, where u_i runs over words from q_0 to a state not in $[q_0]$ such that $\delta(q_0, v) \in [q_0]$ for every proper prefix v of u_i and such that w is not a prefix of u_i; $\mathcal{L}_i$ is the set of words u such that $\delta(q_i, u)$ lies in F, where $q_i = \delta(q, u_i)$. Since there are only finitely many such u_i, this is a finite disjoint union. Observe that $\mathcal{L}_i$ is accepted by the automaton

$$\Gamma_i = (Q \setminus [q_0], \Sigma, \delta, q_i, F \setminus [q_0]) \, ,$$

where we restrict δ to $(Q \setminus [q_0]) \times \Sigma$. Then by the induction hypothesis, each $\mathcal{L}_i$ has the desired form and we can now use the expression

$$\mathcal{L} = \mathcal{L}_0 \cup \bigcup_i w^* u_i \mathcal{L}_i$$

to obtain the result.

□

Although Proposition 22 already implies the statement of Theorem 23, it is possible to give a proof of this well-known dichotomy using linear algebra and a gap result on the norms of semigroup of matrices (see [6]). We will first need to prove a couple of lemmas on counting functions and to do that we introduce some more notions from automata theory.

Definition 26. A sequence $\{f(n)\}_n$ taking values in an abelian group A is called *k-regular* if the elements of its k-kernel generate a finitely generated subgroup of $A^{\mathbb{N}}$. That is, every element in the k-kernel can be written as an integer linear combination of a finite set of A-valued sequences.

Given a subset S of natural numbers, the counting function $\pi_S(n) = \#\{j \leq n \colon j \in S\}$ can be considered as a sequence in the abelian group $(\mathbb{Z}, +)$.

Lemma 27. *If S is a k-automatic subset of $\mathbb{N}$, then $\{\pi_S(n)\}_{n \geq 0}$ is a k-regular sequence.*

Proof. Allouche and Shallit [2, Theorem 16.4.1] prove a more general property. They show that if $a(n)$ and $b(n)$ are two k-regular sequences, then the convolution

$$c(n) := \sum_{i=0}^{n} a(i)b(n-i)$$

is again k-regular. Since $\{\chi_S(n)\}_n$, the characteristic sequence of n, is k-automatic, it is k-regular. Similarly, the constant sequence of all ones is k-regular, and since $\{\pi_S(n)\}_n$ is the convolution of these two sequences, we see that $\{\pi_S(n)\}_n$ is also k-regular.

□

The fact that k-regularity allows one to associate a finitely generated abelian group to a sequence allows one to give a characterization of regularity in terms of matrices as follows. This matrix presentation of a given sequence will help us prove Theorem 23 by using a gap result for the norms of semigroups of matrices.

Lemma 28. *Let $f(n)$ be a sequence taking values in a commutative ring R. If $f(n)$ is k-regular, then there exist matrices $M_0, M_1, M_2, \ldots, M_{k-1}$ with integer entries and vectors v, w with entries in R such that*

$$f(n) = w^T M_{n_1} M_{n_2} \cdots M_{n_s} v$$

for all n, where $(n)_k = n_s \ldots n_2 n_1 \in \Sigma_k^*$.

Proof. Since $f(n)$ is k-regular, its k-kernel generates a finitely generated subgroup of $R^{\mathbb{N}}$. We let $\{\{f_1(n)\}_n, \{f_2(n)\}_n, \ldots, \{f_d(n)\}_n\}$ be a set of generators, which we may assume are elements of the k-kernel. Without loss of generality, we assume that $f_1(n) = f(n)$. Then every subsequence of the form $\{f(k^a n + b)\}_n$ with $0 \leq b < k^a$ can be written as a $\mathbb{Z}$-linear combination of members of the generating set. Let $v_n = (f(n), f_2(n), \ldots, f_d(n))^T$. Then as each $f_i(kn + b)$ for $0 \leq b < k$ will be an integer linear combination of the $f_i(n)$'s, for each b there exists a matrix M_b such that $v_{kn+b} = M_b v_n$ for $n \geq 0$. Then by induction, for $(n)_k = n_s \ldots n_2 n_1$ with $n_i \in \Sigma_k$, we have $v_n = M_{n_1} M_{n_2} \cdots M_{n_s} v_0$. Then we can set $w = (1, 0, 0, \ldots, 0)^T$ and $v := v_0$. This gives $f(n) = w^T M_{n_1} M_{n_2} \cdots M_{n_s} v$. □

Another arithmetical property of the counting function of a k-automatic set that follows from this characterization of k-regularity is the following.

Lemma 29. *Let S be a k-automatic subset of $\mathbb{N}$. Then $a(n) := \pi_S(k^n)$ satisfies a linear recurrence relation.*

Proof. Since $\{\pi_S(n)\}_n$ is a k-regular sequence taking values in $\mathbb{Z}$, by Lemma 28 there exist matrices $A_0, \ldots, A_{k-1}$ and vectors v and w with integer entries such that $\pi_S(k^n) = \pi_S([10^n]_k) = w^T A_0^n A_1 v$. The result now follows from the Cayley-Hamilton theorem applied to A_0. □

Using k-regularity of $\{\pi_S(n)\}$ we obtain another proof of Theorem 23. Since we will look at the growth of the functions and will use a description involving matrices and vectors, we introduce some notation.

Notation 30. *For a $d \times 1$ vector $v = (v_1, v_2, \ldots, v_d)^T$ whose entries are integers, we write $|v| := \sqrt{v_1^2 + v_2^2 + \cdots + v_d^2}$.*

Proof of Theorem 23. By Lemma 27, $\pi_S(n)$ is k-regular. So by Lemma 28, there exist $d \times d$ matrices $A_0, \ldots, A_{k-1}$ with integer entries and integer vectors v, w such that $\pi_S(n) = w^T A_{a_1} \ldots A_{a_s} v$ where $(n)_k = a_s \ldots a_1$, with $a_1, \ldots, a_s \in \Sigma_k$.

Denote by $\mathcal{S} = \langle A_0, \ldots, A_{k-1} \rangle \subseteq \mathcal{M}_d(\mathbb{Z})$ the semigroup generated by the matrices $A_0, \ldots, A_{k-1}$. We may assume without loss of generality that $w^T \mathcal{S}$ spans the space of $1 \times d$ row vectors: if not, we let W denote the subspace spanned by $w^T \mathcal{S}$ and since $\mathcal{S}$ is closed under right-multiplication by $A_0, \ldots, A_{k-1}$, for $i = 0, \ldots, k-1$ we have a map $\tilde{A}_i : W \to W$ given by

$$x \in W \mapsto x A_i.$$

Then after fixing a basis for W this gives us a representation of our semigroup that again generates the counting function π_S. Similarly, we may assume that $\mathcal{S} v$ spans the space of $d \times 1$ column vectors.

Recall that there is an operator matrix norm $\| \cdot \|$ defined on complex matrices, given by $\|A\| = \sup |Au|$, where the supremum is taken over all vectors u with $|u| = 1$. If every matrix in $\mathcal{S}$ has all of its eigenvalues on or inside the unit circle then by [6] we have $\max\limits_{0 \leq a_1, \ldots, a_s \leq k-1} \|A_{a_1} \ldots A_{a_s}\| = \mathrm{O}(s^{d-1})$, and so all entries are polynomially bounded in s. Then $\pi_S(n) = \mathrm{O}(s^{d-1})$ since w and v are constant vectors. Since $s = \mathrm{O}(\log(n))$, we have the first part of the dichotomy.

Alternatively, if there is some matrix in $\mathcal{S}$ that does not have all of its eigenvalues on or inside the unit circle, then by the gap result again in [6], we have that there is some constant c with $|c| > 1$ and some matrix

$$B := A_{t_1} \cdots A_{t_r}$$

in $\mathcal{S}$ such that B has an eigenvalue equal to c. Now we pick a nonzero vector u_1 such that $Bu_1 = cu_1$, and we pick a row vector u_2^T with $u_2^T u_1 = 1$.

Now by assumption, $w^T \mathcal{S}$ spans the space of column vectors, so there are fixed elements $U_1, \ldots, U_d \in \mathcal{S}$ and scalars $\lambda_1, \ldots, \lambda_d$ such that

$$\sum_i \lambda_i w^T U_i = u_2.$$

Similarly, there are $U_1', \ldots, U_d' \in \mathcal{S}$ and scalars $\gamma_1, \ldots, \gamma_d$ such that

$$\sum \gamma_i U_i' v = u_1.$$

Then for $n \geq 1$

$$c^n = u_2^T B^n u_1 = \sum_{i,j} \lambda_i \gamma_j w^T U_i B^n U_j' v.$$

Thus if we let R denote the maximum of $|\lambda_i| \cdot |\gamma_j|$, then for each n there exist (i, j) depending on n such that

$$|w^T U_i B^n U_j v| \geq \frac{|c|^n}{(d^2 R)}.$$

In particular, if we let a denote the maximum of the lengths of the elements U_k and U_ℓ' for $1 \leq k, \ell \leq d$ as products of $A_0, \ldots, A_{k-1}$ then we see that for each n there is some word w_n whose length is at least rn and at most $rn + 2a$ such that

$$\pi_S([w_n]_k) \geq \frac{|c|^n}{(d^2 R)}.$$

As $\pi_S(k^{rn+2a}) \geq \pi_S([w_n]_k)$, we see that

$$\pi_S(k^{rn+2a}) \geq \frac{|c|^n}{(d^2 R)}.$$

But now if N is a positive integer, then there exists some n such that

$$k^{rn+2a} \leq N < k^{r(n+1)+2a},$$

and so

$$\pi_S(N) \geq \frac{|c|^n}{d^2 R}.$$

Since $|c| > 1$, there is some $\alpha \in \mathbb{R}$ such that $|c|^\alpha > k^r$, and so we see that $|c|^n / d^2 R > N^{1/\alpha}$ for N sufficiently large and so we have the other part of the dichotomy.

□

Now we have proved a dichotomy for a k-automatic set. It is either sparse (i.e. the counting function of the set grows at the rate of a positive power of $\log(n)$), or the counting function grows at least as fast as n^α for some $\alpha > 0$.

We also mention here how sparseness of sets relate to density of sets. We first define what we mean by density.

Definition 31. Let S be a subset of $\mathbb{N}$. We define the *density* of S by

$$\lim_{n\to\infty} \frac{\pi_S(n)}{n}, \text{ if exists.}$$

In other words, for any interval $I_n := [0,n] \cap \mathbb{Z}$, $n \in \mathbb{N}$, the density of S, if it exists, is defined by $\lim\limits_{n\to\infty} \dfrac{|S \cap I_n|}{|I_n|}$, where $|S \cap I_n|$ and $|I_n|$ denote the number of elements in sets $S \cap I_n$ and I_n, respectively. Although the density need not exist in general, there are related quantities that always exist. The *lower density* and the *upper density* of S are defined by

$$\liminf_{n\to\infty} \frac{|S \cap I_n|}{|I_n|} \text{ and } \limsup_{n\to\infty} \frac{|S \cap I_n|}{|I_n|},$$

respectively.

We look at a statement that connects sparseness and density of a set.

Proposition 32. *If $S \subseteq \mathbb{N}$ is a k-automatic sparse set then it has upper density (and therefore density and lower density) zero.*

Proof. Since S is sparse there exists $d \geq 1$ such that $\pi_S(n) = \mathrm{O}(\log(n)^d)$. Then $|S \cap [0,n]| \leq C\log(n)^d$ for some $C > 0$ for n large, and since we have $\limsup\limits_{n\to\infty} \dfrac{\log(n)^d}{n} = 0$, the result follows. □

An interesting feature of Proposition 22 combined with Lemma 25 is that it shows that a sparse language $\mathcal{L}$ is a finite disjoint union of languages of the form $v_1 w_1^* v_2 w_2^* \dots v_s w_s^* v_{s+1}$ where $s \geq 0$ and the v_i are possibly trivial words and the w_i are non-trivial words. We shall call languages of this special form *simple sparse languages*.

Then every sparse language is a finite union of disjoint simple sparse languages and if one translates Lemma 25 into sparse k-automatic sets, we see that a sparse k-automatic set can be written as a disjoint union

$$S = S_1 \sqcup S_2 \sqcup \dots \sqcup S_d \tag{2.5}$$

for some integer $d \geq 1$, where each S_i is a set of natural numbers of the form

$$\{[v_1 w_1^{n_1} v_2 w_2^{n_2} \dots v_s w_s^{n_s} v_{s+1}]_k \colon n_1, n_2, \dots, n_s \geq 0\}. \tag{2.6}$$

We call a set of natural numbers of the form in Equation 2.6 a *simple sparse* k-automatic set. Sparse sets are related to *p-normal sets* in [18] and simple sparse sets coincide with the sets

$$U_p(v_{s+1}, v_s, \dots, v_1; w_s, \dots, w_1)$$

that are defined in [18, Definition 7.8].

A straightforward computation involving geometric series gives the following lemma.

Lemma 33. *Let $k \geq 2$ be a natural number and let S be a non-empty simple sparse k-automatic set. Then there exist $s \geq 0$, $c_0, \ldots, c_s \in \mathbb{Q}$ such that $(k^\ell - 1)c_i \in \mathbb{Z}$ for some $\ell \geq 0$, $c_0 + c_1 + \cdots + c_s \in \mathbb{Z}_{\geq 0}$ and positive integers $\delta_1, \ldots, \delta_s$ such that*

$$S = \left\{c_0 + c_1 k^{\delta_s n_s} + c_2 k^{\delta_s n_s + \delta_{s-1} n_{s-1}} \cdots + c_s k^{\delta_s n_s + \cdots + \delta_1 n_1} \colon n_1, \ldots, n_s \geq 0\right\}. \tag{2.7}$$

Moreover $n \geq c_0$ for all $n \in S$ and $c_0 \in S$ if and only if $s = 0$.

Proof. Let $[v_i]_k = a_i$ for $i = 1, \ldots, s+1$ and $[w_i]_k = b_i$ for $i = 1, \ldots, s$. Note that each b_i is strictly positive since the w_i are non-trivial words. Let $\mu_i = \text{length}(v_i) \geq 0$ and $\delta_i = \text{length}(w_i) \geq 1$. Then we compute the value of $[v_1 w_1^{n_1} v_2 w_2^{n_2} \cdots v_s w_s^{n_s} v_{s+1}]_k$ as follows.

$$\begin{aligned}
&[v_1 w_1^{n_1} v_2 w_2^{n_2} \cdots v_s w_s^{n_s} v_{s+1}]_k = a_{s+1} + k^{\mu_{s+1}} \left(b_s + k^{\delta_s} b_s + \cdots + k^{\delta_s(n_s - 1)} b_s\right) + k^{\mu_{s+1} + n_s \delta_s} a_s \\
&+ k^{\mu_{s+1} + \mu_s + n_s \delta_s} \left(b_{s-1} + k^{\delta_{s-1}} b_{s-1} + \cdots + k^{\delta_{s-1}(n_{s-1} - 1)} b_{s-1}\right) + \cdots \\
&+ k^{\mu_{s+1} + \mu_s + \mu_{s-1} + \cdots + \mu_2 + n_s \delta_s + \cdots + n_2 \delta_2} \left(b_1 + k^{\delta_1} b_1 + \cdots + k^{\delta_1(n_1 - 1)} b_1\right) \\
&+ a_1 k^{\mu_{s+1} + \cdots + \mu_2 + \delta_s n_s + \cdots + \delta_1 n_1} \\
&= a_{s+1} + k^{\mu_{s+1}} b_s \left(\frac{k^{n_s \delta_s} - 1}{k^{\delta_s} - 1}\right) + k^{\mu_{s+1} + n_s \delta_s} a_s + k^{\mu_{s+1} + \mu_s + n_s \delta_s} b_{s-1} \left(\frac{k^{\delta_{s-1} n_{s-1}} - 1}{k^{\delta_{s-1}} - 1}\right) + \cdots \\
&+ k^{\mu_{s+1} + \mu_s + \cdots \mu_2 + n_s \delta_s + \cdots + n_2 \delta_2} b_1 \left(\frac{k^{\delta_1 n_1} - 1}{k^{\delta_1} - 1}\right) + a_1 k^{\mu_{s+1} + \mu_s + \cdots + \mu_2 + n_s \delta_s + \cdots + n_1 \delta_1}.
\end{aligned}$$

The result follows, taking $c_0 := a_{s+1} - \frac{k^{\mu_{s+1}} b_s}{k^{\delta_s} - 1}$,

$$c_1 := \frac{k^{\mu_{s+1}} b_s}{k^{\delta_s} - 1} + k^{\mu_{s+1}} a_s - \frac{k^{\mu_{s+1} + \mu_s} b_{s-1}}{k^{\delta_{s-1}} - 1}, \ldots, c_s := a_1 k^{\mu_{s+1} + \mu_s + \cdots + \mu_2} + \frac{k^{\mu_{s+1} + \mu_s + \cdots + \mu_2} b_1}{k^{\delta_1} - 1}.$$

We observe that if $s \geq 1$ then $c_0 < a_{s+1} = [v_{s+1}]_k$ and since every element of S is at least as large as $[v_{s+1}]_k$ we then see that $n \geq c_0$ for every $n \in S$ and $c_0 \in S$ if and only if $s = 0$. Taking $n_1 = n_2 = \cdots = n_s = 0$ and using the fact that S consists of nonnegative integers, we see that $c_0 + \cdots + c_s \in \mathbb{Z}_{\geq 0}$. □

2.3 Christol's Theorem and Kedlaya's Extension

Christol's theorem is a fundamental result that gives a characterization of the collection of algebraic power series with coefficients in a finite field in terms of automatic sequences. Although Christol's theorem gives some of the algebraic elements over a function field, it doesn't give a description of its full algebraic closure. Kedlaya gave a full characterization by passing to generalized series and generalizing p-automaticity to p-quasi-automaticity. We overview Christol's theorem and Kedlaya's generalization in this section. As these characterizations both involve algebraic properties, we start by giving some basic algebraic preliminaries. We assume that the reader is familiar with the ring of formal power series over a field. Given a field $\Bbbk$, we let $\Bbbk[[x]]$ denote the ring of formal power series with coefficients in $\Bbbk$.

Definition 34. Given a field $\Bbbk$, a power series $F(t) \in \Bbbk[[t]]$ is an *algebraic power series* if there exists some $d \geq 1$ and $C_0(t), C_1(t), \ldots, C_d(t) \in \Bbbk[t]$, not all zero, such that

$$C_d(t)F(t)^d + \cdots + C_1(t)F(t) + C_0(t) = 0.$$

Equivalently, $F(t)$ is a power series that is algebraic over the field of rational functions $\Bbbk(t)$. The collection of algebraic power series forms a ring and it contains the power series expansions of rational functions that are regular at $t = 0$. We now state the famous result of Christol [14, 15].

Theorem 35 (Christol)**.** *Let $F(t) = \sum_{n\geq 0} f(n)t^n \in \mathbb{F}_q[[t]]$ be a formal power series where $q = p^a$ for some integer $a \geq 1$ and a prime number p. Then F is an algebraic power series if and only if the sequence $f(n)$ is p-automatic.*

We provide some examples before presenting the proof.

We have seen that the Thue-Morse sequence is 2-automatic in two different ways already: by explicitly writing the finite-state machine that generates it and looking at its 2-kernel and observing that it is finite. Now, by using Christol's theorem, we can use the automaticity of this sequence to show algebraicity of a power series, or, we can prove its automaticity by showing the algebraicity of the series whose coefficient sequence is taken as the Thue-Morse sequence.

Example 36. [Thue-Morse example via Christol's Theorem] Consider the formal power series $F(t) = \sum_{n\geq 0} f(n)t^n$ with coefficients in $\mathbb{F}_2$, where $f(n)$ represents the Thue-Morse sequence; i.e. $f(n)$ is equal to 1 if the binary expansion of n contains odd number of 1's and $f(n) = 0$ if the binary expansion of n has even number of 1's. Then we have the following relations from Equation 2.3:

$$\begin{aligned} f(0) &= 0, \\ f(2n) &= f(n), \\ f(2n+1) &= 1 - f(n). \end{aligned}$$

Using these relations we rewrite the series as

$$\begin{aligned} F(t) &= \sum_{n\geq 0} f(n)t^n = \sum_{n\geq 0} f(2n)t^{2n} + \sum_{n\geq 0} f(2n+1)t^{2n+1} \\ &= \sum_{n\geq 0} f(n)t^{2n} + \sum_{n\geq 0} (1-f(n))t^{2n+1} \\ &= \sum_{n\geq 0} f(n)t^{2n} + \sum_{n\geq 0} (1+f(n))t^{2n+1} \\ &= \sum_{n\geq 0} f(n)\left(t^2\right)^n + t\sum_{n\geq 0} \left(t^2\right)^n + t\sum_{n\geq 0} f(n)\left(t^2\right)^n \\ &= F(t^2) + \frac{t}{1-t^2} + t\,F(t^2) \end{aligned}$$

Rearranging, and using the fact that we are in characteristic 2, we get the following polynomial equation:

$$(1+t)^3F^2 + (1+t)^2F + t = 0 \tag{2.8}$$

This means F satisfies an equation over $\mathbb{F}_2(t)$ with $C_2(t) = (1+t)^3$, $C_1(t) = (1+t)^2$ and $C_0(t) = t$ as in Definition 34, which means $F \in \mathbb{F}_2[[t]]$ is algebraic over $\mathbb{F}_2(t)$.

Another example comes from considering a series whose coefficient sequence is the characteristic function of the set of powers of p, which we know is a p-automatic set.

Example 37. Let us consider the series $G(t) := \sum_{n\geq 0} t^{p^n} \in \mathbb{F}_p[[t]]$, with p a prime number. A simple calculation shows that $G^p = G - t$. i.e. the formal power series G satisfies an equation as in Definition 34 with $C_2(t) = 1 = -C_1(t)$ and $C_0(t) = t$, and hence is algebraic over $\mathbb{F}_p(t)$.

Now we provide some background information to prove Christol's theorem. The proof uses Cartier operators and an equivalent description of algebraicity of power series over $\mathbb{F}_q(t)$.

First, we introduce the Cartier operators and look at some of their arithmetical properties.

Definition 38. Let q be a power of a prime p. For $0 \leq r < q$, a linear transformation $\Lambda_r : \mathbb{F}_q[[t]] \to \mathbb{F}_q[[t]]$ given by

$$\Lambda_r\left(\sum_{n\geq 0} f(n)t^n\right) = \sum_{n\geq 0} f(qn+r)t^n$$

is called the *rth-Cartier operator*.

A useful property of the Cartier operators, which is also used in the proof of Ore's lemma (see Lemma 41), is the following.

Lemma 39. *Let* $F := \sum_{n\geq 0} f(n)t^n$ and $G := \sum_{k\geq 0} g(k)t^k$ *be two formal power series in* $\mathbb{F}_q[[t]]$. *Then the Cartier operators have the following properties:*

(i) $F(t) = \sum_{0\leq r<q} t^r \Lambda_r(F(t))^q$;

(ii) $\Lambda_r(F^qG) = F\,\Lambda_r(G)$ *for* $r = 0, \ldots, q-1$.

Proof. (i) We have

$$\begin{aligned} F(t) = \sum_{n\geq 0} f(n)t^n &= \sum_{0\leq r<q}\sum_{n\geq 0} f(qn+r)t^{qn+r} \\ &= \sum_{0\leq r<q} t^r \sum_{n\geq 0} f(qn+r)t^{nq} \\ &= \sum_{0\leq r<q} t^r \left(\sum_{n\geq 0} f(qn+r)t^n\right)^q \\ &= \sum_{0\leq r<q} t^r \left(\Lambda_r(F(t))\right)^q . \end{aligned}$$

(ii) We have

$$\begin{aligned}
\Lambda_r(F^q G) &= \Lambda_r\left(\left(\sum_{n\geq 0} f(n)t^n\right)^q \left(\sum_{k\geq 0} g(k)t^k\right)\right)\\
&= \Lambda_r\left(\left(\sum_{n\geq 0} f(n)t^{qn}\right) \left(\sum_{k\geq 0} g(k)t^k\right)\right)\\
&= \Lambda_r\left(\sum_{j\geq 0} t^j \left(\sum_{\substack{n,k\geq 0,\\ qn+k=j}} f(n)g(k)\right)\right)\\
&= \sum_{j\geq 0} t^j \left(\sum_{\substack{n,k\geq 0,\\ qn+k=qj+r}} f(n)g(k)\right)\\
&= \sum_{j\geq 0} t^j \left(\sum_{0\leq n\leq j} f(n)g(q(j-n)+r)\right)\\
&= \sum_{n\geq 0} f(n)t^n \left(\sum_{j\geq n} g(q(j-n)+r)t^{j-n}\right)\\
&= \left(\sum_{n\geq 0} f(n)t^n\right)\left(\sum_{k\geq 0} g(qk+r)t^k\right)\\
&= F\,\Lambda_r(G).
\end{aligned}$$

□

Another useful property of Cartier operators is the following.

Lemma 40. *Let $\{f(n)\}_{n=0}^{\infty}$ be a sequence over $\mathbb{F}_q$. Then $\{f(n)\}_n$ is q-automatic if and only if there exists a finite collection of formal power series $\mathcal{F}$ such that*

(a) $F \in \mathcal{F}$, where $F(t) := \sum_{n\geq 0} f(n)t^n$; and

(b) for all $G \in \mathcal{F}$ and $0 \leq r < q$, we have $\Lambda_r(G) \in \mathcal{F}$.

Proof. Suppose $\{f(n)\}$ is q-automatic. Then we know that its q-kernel is finite. Let $K_q = \{\{f_1\}_n, \{f_2\}_n, \ldots, \{f_r\}_n\}$ be its q-kernel with $f_1 = f$. Let $\mathcal{F}$ denote the collection of power series of the form $\sum\limits_{n\geq 0} f_i(n)t^n$ for $1 \leq i \leq r$. Then $F(t) \in \mathcal{F}$. For any $G \in \mathcal{F}$, $G(t) = \sum\limits_{n\geq 0} f_i(n)t^n$ for some $1 \leq i \leq r$. Applying the rth Cartier operator to G, $\Lambda_r(G) = \sum\limits_{n\geq 0} f_i(qn+r)t^n \in \mathcal{F}$. Since $\{f_i(qn+r)\}_n$ corresponds to one of $\{f_j(n)\}_{n\geq 0}$ for $1 \leq j \leq r$ (by definition of q-kernel), $\Lambda_r(G) \in \mathcal{F}$.

If there exists a finite collection of formal power series $\mathcal{F}$ such that $F(t) \in \mathcal{F}$ and $\mathcal{F}$ is closed under the Cartier operators, then any formal power series whose coefficients are taken from K_q is going to be in $\mathcal{F}$. So $|K_q| \leq |\mathcal{F}| < \infty$ since $\mathcal{F}$ is a finite collection. So the q-kernel is finite and $\{f(n)\}_{n=0}^{\infty}$ is q-automatic. □

An equivalent formulation of algebraicity of formal power series (Definition 34) is given by Ore's lemma. This characterization is used in the proof of Christol's theorem.

Lemma 41 (Ore's lemma)**.** *Let $F \in \mathbb{F}_q[[t]]$, $q = p^n$. Then F is algebraic over $\mathbb{F}_q(t)$ if and only if there exist an integer $d \geq 1$ and polynomials $C_0(t), C_1(t), C_2(t), \ldots, C_d(t) \in \mathbb{F}_q[t]$, not all zero, such that*

$$C_0F + C_1F^q + C_2F^{q^2} + \cdots + C_dF^{q^d} = 0.$$

Furthermore, we can assume that $C_0 \not\equiv 0$, i.e. the function $C_0(t)$ is not the constant zero function.

Proof. Suppose F is algebraic over $\mathbb{F}_q(t)$. Let d be the degree of its minimal polynomial. Then $F, F^q, F^{q^2}, \ldots, F^{q^d}$ cannot be linearly independent over $\mathbb{F}_q(t)$. Hence there exists a nontrivial linear relation

$$C_0F + C_1F^q + \cdots + C_dF^{q^d} = 0$$

where $C_0, C_1, \ldots, C_d \in \mathbb{F}_q[t]$. The other direction follows trivially.

Now it remains to show that we can in fact assume $C_0 \not\equiv 0$. Pick a nontrivial relation of the form

$$C_0F + C_1F^q + C_2F^{q^2} + \cdots + C_dF^{q^d} = 0$$

with a minimal d. Let j be the smallest nonnegative integer such that $C_j(t) \not\equiv 0$. Assume towards a contradiction that $j \neq 0$. Since $C_j \in \mathbb{F}_q[t]$ and $\mathbb{F}_q[t] \subseteq \mathbb{F}_q[[t]]$, by (i) in Lemma

39, we get

$$C_j(t) = \sum_{0\le r<q} t^r \left(\Lambda_r(C_j(t))\right)^q .$$

This means that there exists r such that $\Lambda_r(C_j(t)) \not\equiv 0$. Since j is the smallest nonnegative integer with $C_j(t) \not\equiv 0$, we get

$$\sum_{0\le i\le d} C_i F(t)^{q^i} = \sum_{j\le i\le d} C_i F(t)^{q^i} = 0.$$

Applying the rth-Cartier operator we get

$$\sum_{j\le i\le d} \Lambda_r \left(C_i(t) F^{q^i}(t) \right) = 0.$$

By assumption, $j \neq 0$ so we can use (ii) in Lemma 39. Then

$$\sum_{j\le i\le d} \Lambda_r \left(C_i\right) F^{q^{i-1}} = 0.$$

So we obtain a new nontrivial linear relation which contradicts minimality of d. Hence $j = 0$. □

Now we are ready to prove Theorem 35.

Proof of Christol's theorem. If $F(t) = \sum_{n\ge 0} f(n)t^n$ is algebraic over $\mathbb{F}_q(t)$, then there exist an integer $d \ge 1$ and polynomials $C_0(t), C_1(t), \ldots, C_d(t)$ such that

$$C_0(t)F(t) + C_1 F(t)^q + \cdots + C_d F(t)^{q^d} = 0 \tag{2.9}$$

with $C_0(t) \not\equiv 0$, by Lemma 41. Dividing both sides by C_0^2 in Equation 2.9, we get

$$\frac{F}{C_0} + \frac{C_1}{C_0^2}F^q + \cdots + \frac{C_d}{C_0^2}F^{q^d} = 0.$$

Multiplying and dividing the ith term by $C_0^{q^i}$ for $2 \le i \le d$, we get

$$\frac{F}{C_0} + \frac{C_1 C_0^q}{C_0^2 C_0^q}F^q + \cdots + \frac{C_d C_0^{q^d}}{C_0^2 C_0^{q^d}}F^{q^d} = 0.$$

If we put $G := \frac{F}{C_0}$, we get

$$G + C_1 C_0^{q-2} G^q + \cdots + C_d C_0^{q^d-2} G^{q^d} = 0.$$

From this, we get $G = -\sum_{i=1}^{d} C_i C_0^{q^i-2} G^{q^i}$. Let $B_i := -C_i C_0^{q^i-2}$ for $1 \leq i \leq d$. Then $G = \sum_{i=1}^{d} B_i(X) G^{q^i}$. Now, let $N = \max(\deg C_0, \max_i \deg B_i)$. Let $\mathcal{H}$ denote the collection of formal power series in $\mathbb{F}_q[[t]]$ of the form $\sum_{0\leq i\leq d} D_i G^{q^i}$, with $D_i \in \mathbb{F}_q[t]$ and $\deg D_i \leq N$. Observe that $\mathcal{H}$ is a finite collection because for each i, $\deg D_i \leq N$ and that $F = C_0 G \in \mathcal{H}$ since $\deg C_0 \leq N$ by definition of N. We will use Lemma 40 and show that $\mathcal{H}$ is mapped into itself under each Cartier operator Λ_r. Let $H = \sum_{0\leq i\leq d} D_i G^{q^i} \in \mathcal{H}$. Then

$$\begin{aligned}
\Lambda_r(H) &= \Lambda_r\left(D_0 G + \sum_{1\leq i\leq d} D_i G^{q^i}\right) \\
&= \Lambda_r\left(\sum_{1\leq i\leq d} D_0 B_i G^{q^i} + \sum_{1\leq i\leq d} D_i G^{q^i}\right) \\
&= \Lambda_r\left(\sum_{1\leq i\leq d} (D_0 B_i + D_i) G^{q^i}\right) \\
&= \sum_{1\leq i\leq d} \Lambda_r\left((D_0 B_i + D_i) G^{q^i}\right) \text{ (since } \Lambda_r \text{ is linear)} \\
&= \sum_{1\leq i\leq d} \Lambda_r(D_0 B_i + D_i) G^{q^i-1} \text{ by (ii) in Lemma 39.}
\end{aligned}$$

Now, observe that $\deg D_0 \leq N$ and $\deg D_i \leq N$ for all $1 \leq i \leq t$ by definition of $\mathcal{H}$. Also, $\deg B_i \leq N$ for all $1 \leq i \leq d$ by definition of N. So, we get $\deg(D_0 B_i + D_i) \leq 2N$. Hence,

$$\deg(\Lambda_r(D_0 B_i + D_i)) \leq \frac{2N}{q} \leq N$$

since $q \geq 2$. Therefore, $\{f(n)\}_{n=0}^{\infty}$ is q-automatic and, by Proposition 18, it is p-automatic.

If $f(n)$ is p-automatic, then it is q-automatic by Proposition 18 again. So its q-kernel is finite. Denote the q-kernel by $K_q = \{\{f_1\}_n, \{f_2\}_n, \ldots, \{f_d\}_n\}$ for some integer $d \geq 1$ with $f_1 = f$. For $1 \leq j \leq d$ define $F_j(t)$ to be the power series

$$\sum_{n\geq 0} f_j(n)t^n.$$

Then

$$F_j(t) = \sum_{n\geq 0} f_j(n)t^n = \sum_{0\leq r<q}\sum_{m\geq 0} f_j(qm+r)t^{qm+r}.$$

By assumption, there is some $b(j,r) \in \{1, \ldots, d\}$ such that $f_j(qm+r) = f_{b(j,r)}(m)$ for all m. Then

$$F_j(t) = \sum_{0\leq r<q} t^r F_{b(j,r)}(t)^q.$$

This shows that each $F_j(t)$ is a $\mathbb{F}_q[t]$-linear combination of $F_i(t^q)$'s, $1 \leq i \leq d$. This means each $F_j(t)$ is in the $\mathbb{F}_q(t)$-vector space generated by $F_i(t^q)$, $1 \leq i \leq d$. But then, we similarly have that each $F_j(t^q)$ is in the vector space generated by $F_i(t^{q^2})$, $1 \leq i \leq d$, and hence both $F_j(t)$ and $F_j(t^q)$ are in the vector space generated by $F_i(t^{q^2})$, $1 \leq i \leq d$. Continuing with $F_j(t^{q^2})$, $F_j(t^{q^3})$ and so on (up to $F_j(t^{q^d})$), we get all of $F_j(t), F_j(t^q), F_j(t^{q^2}), \ldots, F_j(t^{q^d})$ are in the $\mathbb{F}_q(t)$-vector space generated by $F_i(t^{q^{d+1}})$, $1 \leq i \leq d$. By dimension counting, there exists a nontrivial relation among $F_j(t), F_j(t^q), F_j(t^{q^2}), \ldots, F_j(t^{q^d})$ since they are $d+1$ power series in a vector space of dimension d. We get the result since this holds for all $1 \leq j \leq d$ and $F_1 = F$, together with Lemma 41. □

An application of Christol's theorem is showing that Hadamard products of algebraic series are algebraic. We provide the definition of Hadamard product below and prove the aforementioned property.

Definition 42. The product $(F \odot G)(t) = \sum_{n\geq 0} (f(n)g(n))\, t^n$ is called the *Hadamard product* of $F(t) = \sum_{n\geq 0} f(n)t^n$ and $G(t) = \sum_{n\geq 0} g(n)t^n$.

We can prove the following by using Christol's theorem and item (ii) in Corollary 15.

Theorem 43. *Let p be a prime number and q be a power of p. If $F, G \in \mathbb{F}_q[[t]]$ are algebraic over $\mathbb{F}_q(t)$, then $F \odot G$ is also algebraic over $\mathbb{F}_q(t)$.*

Proof. Let $F(t) = \sum_{n\geq 0} f(n)t^n$ and $G(t) = \sum_{n\geq 0} g(n)t^n$. Then, since F and G are algebraic over $\mathbb{F}_q(t)$, by Christol's theorem, the sequences $\{f(n)\}_n$ and $\{g(n)\}_n$ are p-automatic. Then by item (ii) in Corollary 15, the sequence $\{f(n)g(n)\}_n$ is p-automatic as well. Applying Christol's theorem again, we get $F \odot G$ is algebraic over $\mathbb{F}_q(t)$. □

Next we define sparse series and also show that, like the collection of algebraic power series, they form a ring under multiplication.

Definition 44. Let p be a prime and let q be a power of p. Given an algebraic power series $F(t) = \sum_{n\geq 0} f(n)t^n \in \mathbb{F}_q[[t]]$, we call the formal power series $F(t)$ a *sparse series* if the support of $F(t)$ is a sparse p-automatic set; that is, if $\{n\colon f(n) \neq 0\}$ is sparse.

We have a similar definition for formal Laurent series, $\mathbb{F}_q((t))$, which is an algebra. Note that $\mathbb{F}_q[[t]] \subseteq \mathbb{F}_q((t))$ as a subring. Algebraic formal power series form a commutative ring as a subset of algebraic Laurent series. We can also show that sparse algebraic series also form a ring.

Lemma 45. *The set of all sparse series forms a commutative ring (as a subset of algebraic Laurent series). i.e. The series in $\mathbb{F}_q[[t]]$ with sparse support form a commutative ring.*

Proof. Denote the set of all sparse series by $\mathcal{S}$. Let $F(t), G(t) \in \mathcal{S}$. Then we can write $F(t) = \sum_{\alpha\in\mathbb{F}_q^*} \alpha \cdot \sum_{n\in S_\alpha} t^n$. Denote $F_{S_\alpha}(t) := \sum_{n\in S_\alpha} t^n$. Similarly, for $G(t)$, we can write $G(t) = \sum_{\beta\in\mathbb{F}_q^*} \beta \cdot \sum_{m\in S_\beta} t^m = \sum_{\beta\in\mathbb{F}_q^*} \beta \cdot G_{S_\beta}(t)$. Here, S_α and S_β are sparse sets. Now, it suffices to show that $F_{S_\alpha}(t) + G_{S_\beta}(t)$ and $F_{S_\alpha}(t)G_{S_\beta}(t)$ have sparse support. We can write

$$F_{S_\alpha}(t) + G_{S_\beta}(t) = \sum_{n\in S_\alpha} t^n + \sum_{m\in S_\beta} t^m = \sum_{n\in S_\alpha\cup S_\beta} t^n + \sum_{n\in S_\alpha\cap S_\beta} t^n$$

and

$$F_{S_\alpha}(t)G_{S_\beta}(t) = \left(\sum_{n\in S_\alpha} t^n\right)\left(\sum_{m\in S_\beta} t^m\right) = \sum_{n\in S_\alpha}\sum_{m\in S_\beta} t^{n+m}.$$

Note that intersection of two sparse sets is sparse since $S' := S_\alpha \cap S_\beta \subseteq S_\alpha$ hence $\pi_{S'}(n) \leq \pi_S(n) = O((\log n)^d)$. Noticing that $\pi_{S_\alpha\cup S_\beta}(n) \leq \pi_{S_\alpha}(n) + \pi_{S_\beta}(n)$, we get that $S_\alpha \cup S_\beta$ is also sparse. Hence $F_{S_\alpha}(t) + G_{S_\beta}(t)$ has sparse support. Note also that

$$\pi_{S_\alpha+S_\beta}(n) \leq \pi_{S_\alpha}(n) \cdot \pi_{S_\beta}(n)$$

where $S_\alpha + S_\beta := \{a+b\colon a \in S_\alpha, b \in S_\beta\}$. So $F_{S_\alpha}(t)G_{S_\beta}(t)$ also has sparse support. The automaticity conditions (which are needed for algebraicity) follow from Corollary 20. $\square$

We will see in Chapter 6 that similar properties hold for generalized sparse sets, i.e. sparse sets that are not only subsets of $\mathbb{N}$ but subsets of a well-ordered subset of rational numbers. For a subset $S \subseteq \mathbb{Q}$, we will say that S is *well-ordered* if every nonempty subset of S has a minimal element. Note that this is equivalent to saying that there is no infinite decreasing sequence $s_1 > s_2 > \cdots$ within S.

Remark 46. *Let A be a well-ordered subset of $\mathbb{Q}$. Then, the following are equivalent:*

(i) Every nonempty subset of A has a minimal element.

(ii) There is no infinite decreasing sequence $a_1 > a_2 > \cdots$ within A.

Proof. For $(i) \implies (ii)$, suppose every nonempty subset of A has a minimal element and that there is an infinite decreasing sequence $a_1 > a_2 > \cdots$ within A. Then $\{a_1, a_2, \ldots\}$ is a subset of A without a minimal element, contradiction. For $(ii) \implies (i)$, suppose there is a nonempty subset S of A without a minimal element. Then for each $s_i \in S$ we can find $s_{i+1} \in S$ such that $s_i > s_{i+1}$ forming an infinite decreasing sequence within S, which is within A. $\square$

Kedlaya [28] used generalized power series (see Hahn [26]) to give an extension of Christol's theorem, which has the advantage of giving a complete automaton-theoretic description of the algebraic closure of $\mathbb{F}_q(t)$. Here we give a brief introduction to the concepts involved. Let $\Bbbk$ be a field. We define the collection of *generalized Laurent series* over $\Bbbk$ to be the set of elements of the form $\sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha$, where $f : \mathbb{Q} \to \Bbbk$ has the property that $\{\alpha\colon f(\alpha) \neq 0\}$ is a well-ordered subset of $\mathbb{Q}$, where we use the usual order $<$ on $\mathbb{Q}$. Restricting to maps f with well-ordered support allows us to endow the set of generalized Laurent series over $\Bbbk$ with a ring structure, where addition and multiplication are given respectively by

$$\sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha + \sum_{\alpha \in \mathbb{Q}} g(\alpha)t^\alpha = \sum_{\alpha \in \mathbb{Q}} (f+g)(\alpha)t^\alpha$$

and

$$\left(\sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha\right)\left(\sum_{\alpha \in \mathbb{Q}} g(\alpha)t^\alpha\right) = \sum_{\alpha \in \mathbb{Q}}\left(\sum_{\beta\gamma=\alpha} f(\beta)g(\gamma)\right)t^\alpha.$$

We refer the reader to Kedlaya [28, 29] for further information.

If the support is contained in $\mathbb{Q}_{\geq 0}$, that is the set of rational numbers greater than or equal to zero, then we call f a *generalized power series*. We let $\Bbbk((t^{\mathbb{Q}}))$ denote the set of generalized Laurent series over the field $\Bbbk$, and we let $\Bbbk[[t^{\mathbb{Q}}]]$ denote the set of generalized power series over $\Bbbk$. The generalized power series over $\Bbbk$ form a local ring with unique maximal ideal consisting of generalized power series $\sum\limits_{\alpha \geq 0} f(\alpha)t^{\alpha}$ with $f(0) = 0$. We let $\Bbbk[[t^{\mathbb{Q}}]]_{>0}$ denote this maximal ideal. It is convenient to let $\Bbbk((t^{\mathbb{Q}}))_{<0}$ denote the collection of generalized Laurent series over k whose support lies in $(-\infty, 0)$. We now give further details concerning Kedlaya's automaton-theoretic characterization of the algebraic closure of $\mathbb{F}_p(t)$.

Let $k \geq 2$ be a natural number and let $\Sigma^* := \{0, 1, \ldots, k-1, \bullet\}^*$. We say that a string $u = u_1 \ldots u_n \in \Sigma^*$, with $\bullet$ representing the radix point, is a *valid* base-k expansion, if $n \geq 1$, $u_1 \neq 0$, $u_n \neq 0$ and exactly one of $u_1, \ldots, u_n$ is equal to the radix point. If $u = u_1 \ldots u_n$ is a valid base-k expansion and u_j is its radix point, then we can associate a nonnegative k-adic rational, $[u]_k$, to u via the rule

$$[u]_k = \sum_{i=1}^{j-1} u_i k^{j-1-i} + \sum_{i=j+1}^{n} u_i k^{j-i}. \tag{2.10}$$

We let

$$S_k := \{m/k^n \colon m, n \in \mathbb{Z}_{\geq 0}\}. \tag{2.11}$$

Given a valid base-k expansion u we obtain a value $[u]_k \in S_k$, where we take $[\,\bullet\,]_k = 0$, and we say that u is the base-k expansion of $[u]_k$. Conversely, given an element of S_k it has a unique valid base-k expansion and for $v \in S_k$, we write $(v)_k$ for the valid base-k expansion of v. Observe that the maps $[\,\cdot\,]_k$ and $(\,\cdot\,)_k$ naturally extend the maps introduced earlier.

A function $f : S_k \to \Delta$ is k-automatic (in Kedlaya's sense) if there is a DFAO M with input alphabet $\Sigma = \{0, 1, 2, \ldots, k-1, \bullet\}$ and output alphabet Δ such that for each $v \in S_k$, $f(v) = f_M((v)_k)$. In analogy with the classical case, a subset of S_k is called a *k-automatic set* if its characteristic function is k-automatic.

Kedlaya's extension of Christol's theorem uses the notion of quasi-automatic series, which we now define.

Definition 47. Let p be a prime and let q be a power of p. A generalized Laurent series $\sum\limits_{\alpha \in \mathbb{Q}} f(\alpha)t^{\alpha} \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is *p-quasi-automatic* if the following hold:

(i) for some integers a and b with $a > 0$, the set $aS + b := \{ai + b \colon i \in S\}$ is contained in S_p; and

(ii) for some a, b for which (i) holds, the function $f_{a,b} : S_p \to \mathbb{F}_q$ given by $f_{a,b}(x) = f\left(\frac{x-b}{a}\right)$ is p-automatic (in the sense given above).

Kedlaya's [28, Theorem 4.1.3] main result is the following extension of Christol's theorem (see also [29, Theorem 10.4]).

Theorem 48. *(Kedlaya) Let p be prime and let $F(t) = \sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha \in \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ be a generalized Laurent series. Then if $F(t)$ is algebraic over $\bar{\mathbb{F}}_p(t)$ then there is a power q of p such that $F(t) = \sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha \in \mathbb{F}_q((t^{\mathbb{Q}}))$ and $F(t)$ is p-quasi-automatic. Conversely, if $F(t) = \sum_{\alpha \in \mathbb{Q}} f(\alpha)t^\alpha \in \mathbb{F}_q((t^{\mathbb{Q}}))$ is p-quasi-automatic then $F(t)$ is algebraic over $\bar{\mathbb{F}}_p(t)$.*

In Theorem 48, $\bar{\mathbb{F}}_p$ denotes the algebraic closure of the field $\mathbb{F}_p$.

Before concluding this section, we would like to mention some results from [28] that were used to prove Theorem 48 by Kedlaya in [28]. Combining the results from Lemma 7.2.1 and Lemma 7.2.2 in [28] we get the following:

Proposition 49. *Let $F, G \in \mathbb{F}_q((t^{\mathbb{Q}}))$.*

(i) If F and G are p-automatic (resp. p-quasi-automatic), Then $F + G$ is p-automatic (resp. p-quasi-automatic).

(ii) If F and G are p-automatic (resp. p-quasi-automatic). Then FG is p-automatic (resp. p-quasi-automatic).

Proposition 49 is used in the proof of Lemma 81 and makes the proof significantly shorter.

2.4 Cobham's Theorem

In this section, we provide an overview of Cobham's (big) theorem[1] [16] and give a recent proof due to Krebs [31]. We also give necessary background for this proof in this section.

[1] This is not Theorem 17

Krebs' proof uses a different approach than the previous proofs of the famous result. The main problem in proving Cobham's (big) theorem is that we want to consider sets of the same numbers in two different integer bases. Krebs gets around this difficulty by enlarging the alphabet.

We now state Cobham's big theorem. We recall that integers $k, \ell > 1$ are *multiplicatively independent* if $k^a = \ell^b$ has no non-trivial integer solutions a, b.

Theorem 50 (Cobham [16])**.** *Let $k, \ell \in \mathbb{N}_{\geq 2}$ be multiplicatively independent. If a sequence in $\mathbb{N}$ is both k-automatic and ℓ-automatic, then it is ultimately periodic.*

We recall the notions of periodic and ultimately periodic for sequences.

Definition 51. A sequence $\{a(n)\}_n$ is *periodic* if there exists an integer $m \geq 1$ such that $a(n) = a(n+m)$ for all $n \geq 0$. In this case, m is said to be a period of the sequence $a(n)$. A sequence $\{a(n)\}_n$ is ultimately periodic if there exist integers $k \geq 1$ and $N \geq 1$, such that $a(n) = a(k+n)$ for all $n \geq N$.

Now we have all the required definitions to understand the statement of Cobham's theorem, we collect background on the methods used by Krebs to prove it. We start by local periods. Local periods are defined on intervals and by an interval we mean an interval of natural numbers. For instance, the interval $[1, 5]$ is equal to $\{1, 2, 3, 4, 5\}$.

Definition 52. A sequence $\{a(n)\}_n$ is said to have *local period* $p > 0$ on an interval $I \subseteq \mathbb{N}$ if $a(n) = a(n+p)$ for all $n \geq 0$ such that n, $n+p \in I$.

In the proof of Cobham's theorem which will be presented in this section, local periods will be used to show ultimate periodicity of the sequence in question. This will be done by proving local periodicity of the sequence on certain intervals and then collecting the intervals while showing that the sequence has a common local period on the union. To this end, we prove a lemma which will be useful. In the statement of the following lemma there is not necessarily a relation between p and q.

Lemma 53. *Let $\{a(n)\}_n$ be a sequence with local period $p > 0$ on an interval $I \subseteq \mathbb{N}$. Suppose $\{a(n)\}_n$ has local period $q > 0$ on an interval $J \subseteq \mathbb{N}$. If $|I \cap J| \geq p + q$, then $\{a(n)\}_n$ has local period p on $I \cup J$.*

Proof. Let $n \in \mathbb{N}$ such that n and $n+p$ are both in $I \cup J$. If n and $n+p$ are both in I, then there is nothing to show. If $n \in I \setminus J$, $n+p \in J \setminus I$, then $p > |I \cap J| \geq p+q$, a contradiction. By the same reasoning, we are done if $n \in J \setminus I$ and $n+p \in I \setminus J$. Therefore we may suppose both n and $n+p$ are in J. We can find an $m \in I \cap J$ such that $m, m+p \in J$ with $m \equiv n \mod q$ since $|I \cap J| \geq p+q$. Now we have $a(n) = a(m)$ by local periodicity of J and $a(m) = a(m+p)$ by local periodicity of I and finally, $a(m+p) = a(n+p)$ by local periodicity of J again, which proves $a(n) = a(n+p)$ for all $n, n+p \in I \cup J$. So $\{a(n)\}_n$ has local period p on $I \cup J$. □

Given a finite subset D of the integers that contains $\Sigma_k = \{0, \ldots, k-1\}$, we can form base-$k$ expansions whose digits lie in D. Given a word $w = d_n \cdots d_0$ over the alphabet D, we then define $[w]_k = \sum_{i=0}^{n} d_i k^i$.

Definition 54. *A sequence $\{a(n)\}_n$ is called (D,k)-automatic if there exists a DFAO $(Q, D, \delta, q_0, \Delta, \tau)$ such that for all $w \in D^*$ with $[w]_k = n$ we have $a(n) = \tau(\delta(q_0, w))$.*

Now we show that Definitions 6 and 54 are equivalent. i.e. k-automaticity and (D,k)-automaticity are equivalent. The procedure that will be described in the following result involves what is commonly referred to as *normalization*. In the proof we follow ideas from [34, Chapt. 7].

Proposition 55. *Let D be a finite set of integers that contains Σ_k. Then a sequence $\{a(n)\}_n$ is (D,k)-automatic (in the sense of Definition 54) if and only if it is k-automatic (in the sense of Definition 6).*

Proof. One direction is trivial because if the automaton works with a larger alphabet that contains Σ_k then that means all the needed arrows/paths are already there, and one can remove the "redundant" transitions from the picture to get the desired result. We show the other direction. Suppose $\{a(n)\}_n$ is k-automatic. Then there exists a DFAO $M = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$ generating $\{a(n)\}_n$. From M we create a new DFAO $M' = (Q', D, \delta', q_0', \Delta, \tau')$ as follows. The input alphabet will be a finite set D containing Σ_k. Since we want this new automaton to generate the same sequence of numbers as the original one but to allow for different representations of natural numbers n, we have to find a way around this. We let m denote the maximum of the absolute values of elements of D and we let $Q' = Q \times \Sigma_k \times \{-m, \ldots, m\}$. This set Q' will be the set of states of our machine and the initial state q_0' is the state $(q_0, 0, 0)$.

We define the transition function $\delta' : Q' \times D \to Q'$ via the rule $\delta'((q,a,j),d) = (\delta(q,j'), j', s)$ for $(q,a,j) \in Q'$ and $d \in D$, where $j' \in \Sigma_k$ satisfies $j' \equiv j + d \pmod{k}$ and $s = (j+d-j')/k$. Observe that $|s| \leq (m+m+k-1)/k < m+1$, since $k \geq 2$, so δ' does indeed map into Q'. Now let $w = d_t \cdots d_0 \in D^*$ and for $i = 0, \ldots, t$, we let

$(v_i, c_i) = \delta'(q_0', d_i \cdots d_0)$. Then each $v_i \in Q'$ is of the form (u_i, a_i, s_i) with $u_i \in Q$, $a_i \in \Sigma_k$ and $s_i \in \{-m, \ldots, m\}$. We show by induction on t that $a_0 + a_1 k + \cdots + a_t k^t + s_t k^{t+1} = [w]_k$ and $\delta'(q_0', w) = (\delta(q_0, a_t \cdots a_0), a_t, s_t)$.

Observe that when $t = 0$, $w = d_0$ and if we let a_0 be the unique element of Σ_k with $d_0 \equiv a_0 \pmod k$ then $\delta'(q_0', d_0) = (\delta(q, a_0), a_0, (d_0 - a_0)/k)$, and so $s_0 = (d_0 - a_0)/k$, which means $a_0 + ks_0 = d_0$, and so we obtain the base case. Suppose now that the claims hold for all words over D of length at most t. Then if $w = d_t \cdots d_0$ is a word of length $t + 1$ and we let $w' = d_{t-1} \cdots d_0$ then by the induction hypothesis, we have $\delta'(q_0', w') = (\delta(q_0, a_{t-1} \cdots a_0), a_{t-1}, s_{t-1})$ and $[w']_k = a_0 + \cdots + a_{t-1}k^{t-1} + s_{t-1}k^t$. Then by the induction hypothesis

$$\delta'(q_0', w) = \delta'(q_0', d_t w') = \delta'((\delta(q_0, a_{t-1} \cdots a_0), a_{t-1}, s_{t-1}), d_t).$$

By definition $a_t \equiv s_{t-1} + d_t \pmod k$ and $s_t = (d_t + s_{t-1} - a_t)/k$. Thus we have

$$\delta'(\delta(q_0, a_{t-1} \cdots a_0), a_{t-1}, s_{t-1}), d_t) = (\delta(q_0, a_t \cdots a_0), a_t, s_t).$$

This then gives the induction step for the first of the two claims. Next observe that

$$a_0 + a_1 k + \cdots + a_t k^t + s_t k^{t+1} = (a_0 + \cdots + a_{t-1}k^{t-1}) + a_t k^t + s_t k^{t+1},$$

and by the induction hypothesis, this is equal to

$$[w']_k - s_{t-1}k^t + a_t k^t + s_t k^{t+1}.$$

Finally, using the fact that $s_t = (d_t + s_{t-1} - a_t)/k$, we see that this is just $[w']_k + d_t k^t = [w]_k$, and so we obtain the claims by induction.

We finally define $\tau' : Q' \to \Delta$ via the rule $\tau'((q, a, s)) = \tau'(\delta(q, (|s|)_k)$ for $q \in Q, a \in \Sigma_k, s \in \{-m, \ldots, m\}$. Notice that if $w = d_t \cdots t_0 \in D^*$ is a word with $[w]_k = n \geq 0$ then by the claim above, $\delta'(q_0', w) = \delta(q_0, a_t \cdots a_0), a_t, s_t)$ for some $a_0, \ldots, a_t \in \Sigma_k$ and some $s_t \in \{-m, \ldots, m\}$ with $n = a_0 + a_1 k + \cdots + a_t k^t + s_t k^{t+1}$. Moreover, since $n \geq 0$ we must have $s_t \geq 0$. Thus by definition $\tau'(\delta(q_0, w)) = \tau(\delta(q_0, (s_t)_k a_t \cdots a_0) = \delta(q_0, (n)_k)$, and so we see that the DFAO M' gives the same output regardless of which expansion over D we pick for a nonnegative integer n and, moreover, the output is equal to $\tau(\delta(q_0, (n)_k))$, the output given by the DFAO M. □

We give an example that illustrates how to construct a (D, k)-DFAO from a given k-DFAO.

Example 56. Let $k = 2$ and consider the example of the k-DFAO given in Figure 2.3. We shall show how to convert this to a (D, k)-DFAO when $D = \{-1, 0, 1\}$. One can follow the procedure given in Proposition 55, but we introduced more states than necessary in the proposition to help with bookkeeping. One can, in this case, work with just four states as shown in the figure below with initial state $[q_0, 0]$.

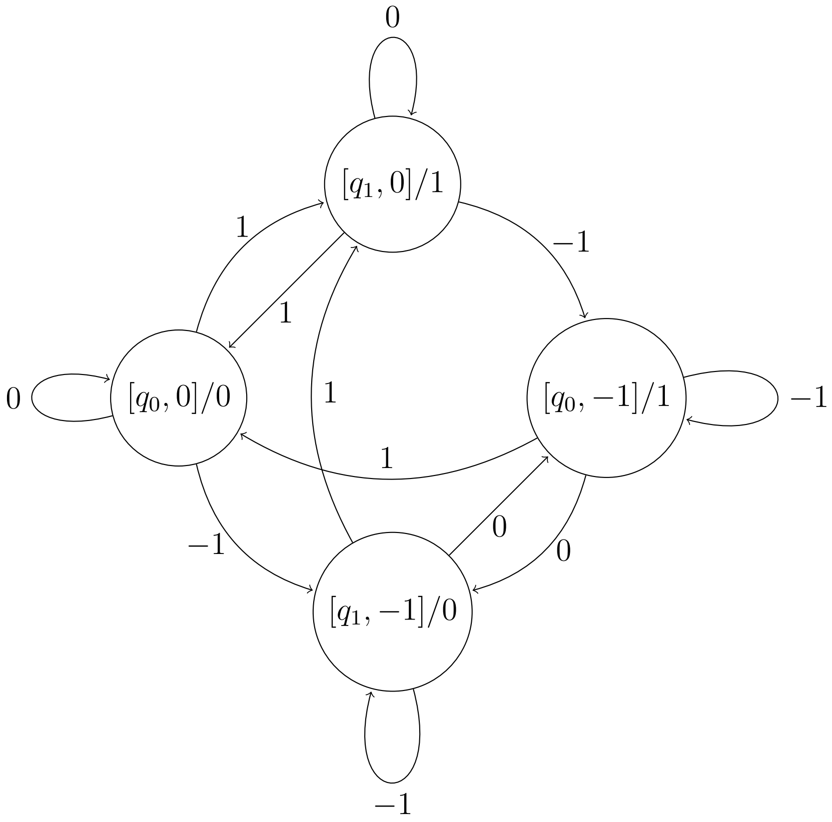

Figure 2.5: A $(\{-1, 0, 1\}, 2)$-DFAO generating the Thue-Morse sequence.

It is an enjoyable exercise for the reader to show that the finite-state machine given in Figure 2.5 takes as input one of the possible base-k expansions of a natural number n over $D = \{-1, 0, 1\}$ and outputs the n-th term of the Thue-Morse sequence, regardless of which expansion of n is selected.

We recall one last very well-known result that is necessary to prove Cobham's Theorem, Dirichlet's approximation theorem.

Theorem 57 (Dirichlet's Theorem)**.** *Let $k, \ell \geq 2$ be two integers. For any real number $\epsilon > 0$, there exist positive natural numbers m and n such that $|k^m - \ell^n| \leq \epsilon \min(k^m, \ell^n)$.*

Proof. [41] Let $\epsilon > 0$ be an arbitrary real number and let $k, \ell \geq 2$ be two integers. We may assume without loss of generality that $k \geq \ell$. We define $a(i) = \lfloor \log_l k^i \rfloor$ for $i \geq 0$ where $\lfloor \cdot \rfloor$ represents the floor function. i.e. the function that returns the greatest integer that is less than or equal to the input number. Then $\{a(i)\}_i$ is a strictly increasing sequence of integers as we assumed $k \geq \ell$. Let t be a positive integer such that $\epsilon > \frac{\ell-1}{t-1}$. Consider the rational numbers $\frac{1}{\ell^{a(0)}}, \frac{k}{\ell^{a(1)}}, \frac{k^2}{\ell^{a(2)}}, \ldots, \frac{k^{t-1}}{\ell^{a(t-1)}} \in [1, \ell)$. By the Pigeonhole Principle, there exist integers $0 \leq i < t$, $0 \leq j < t$ such that $i \neq j$, and

$$\left| \frac{k^j}{\ell^{a(j)}} - \frac{k^i}{\ell^{a(i)}} \right| \leq \epsilon.$$

Without loss of generality, we may assume $i < j$. Then we have

$$\frac{\ell^{a(j)}}{k^i} \left| \frac{k^j}{\ell^{a(j)}} - \frac{k^i}{l^{a(i)}} \right| = |k^{j-i} - \ell^{a(j)-a(i)}| \leq \frac{\ell^{a(j)}}{k^i} \epsilon \leq \epsilon \min(k^{j-i}, \ell^{a(j)-a(i)})$$

since $k \geq \ell \geq 2$ by assumption. Now let $m := j - i$ and $n := a(j) - a(i)$. Since $j > i$, $m > 0$ and since the sequence $\{a(n)\}_n$ is strictly increasing, $n = a(j) - a(i) > 0$ for $j > 0$ as well. □

The proof below of Theorem 50 is due to Krebs [31]. We elaborate on the details of the original proof.

Proof of Theorem 50. Suppose $\{a(n)\}_n$ is both k-automatic and ℓ-automatic for multiplicatively independent $k, \ell \geq 2$. Denote the open and closed balls in $\mathbb{Z}$ centred at $x \in \mathbb{R}$ with radius $r \in \mathbb{R}$ by $B(x; r) := (x - r, x + r) \cap \mathbb{Z}$ and $B[x; r] := [x - r, x + r] \cap \mathbb{Z}$, respectively. For digit sets $B(0; k)$ and $B(0; \ell)$ we will write D_k and D_ℓ, respectively. Now by Proposition 55, since $\{a(n)\}_n$ is k-automatic and ℓ-automatic, it is also (D_k, k)-automatic and (D_ℓ, ℓ)-automatic. So there are two finite automata $M_k = (Q_k, D_k, \delta_k, q_{0,k}, \Delta, \tau_k)$ and $M_\ell = (Q_\ell, D_\ell, \delta_\ell, q_{0,\ell}, \Delta, \tau_\ell)$ that generate $\{a(n)\}_n$. Let $q \in Q_k$, $q' \in Q_\ell$ be two states. We look at all the words over the alphabet D_k that have base-k expansions that are natural numbers and which end at state q; i.e., the language $L_{k,q} = \{w \in D_k^* \colon \delta_k(q_{0,k}, w) = q \text{ and } [w]_k \in \mathbb{N}\}$. Similarly let $L_{\ell,q'}$ be the language $\{w \in D_\ell^* \colon \delta_\ell(q_{0,\ell}, w) = q' \text{ and } [w]_\ell \in \mathbb{N}\}$. Then each of $\{[L_{k,q}]_k \colon q \in Q_k\}$ and $\{[L_{\ell,q'}]_\ell \colon q' \in Q_\ell\}$ is a finite cover of $\mathbb{N}$ since both Q_k and Q_ℓ are finite sets. Observe that for $w \in L_{k,q}$ and $x \in [D_k^n]_k$, $f([wx]_k) = \tau_k(\delta_k(q_{0,k}, wx)) = \tau_k(\delta_k(q, x))$ which means for all $n \geq 0$,

$$f(k^n[w]_k + [x]_k) = f(k^n[w']_k + [x]_k) \tag{2.12}$$

for $w, w' \in L_{k,q}$, $x \in [D_k^n]_k$. Similarly for all $m \geq 0$,

$$f(\ell^m[w]_\ell + [y]_\ell) = f(\ell^m[w']_\ell + [y]_\ell) \tag{2.13}$$

for $w, w' \in L_{\ell,q'}$, $y \in [D_\ell^m]_\ell$. In particular, for each $q \in Q_k$, f is constant on $[L_{k,q}]_k$ and for each $q' \in Q_\ell$, f is constant on $[L_{\ell,q'}]_\ell$. We now want to create local periods and invoke Lemma 53. Let

$$Q_\infty := \{q' \in Q_\ell \colon \#[L_{(\ell,q')}]_\ell = \infty\}.$$

Since the sets $[L_{k,q}]_k$ form a finite cover of $\mathbb{N}$, for each $q' \in Q_\infty$ there exists at least one $q \in Q_k$ such that $[L_{k,q}]_k \cap [L_{\ell,q'}]_\ell$ has at least two elements. For each such (q, q') we pick $x = x_{(q,q')}$ and $y = y_{(q,q')}$ in the intersection with $x > y$. We let $\mathcal{S}$ denote the set of such pairs (q, q') for which the intersection has at least two elements. Notice that since $[L_{(k,q)}]_k \cap [L_{(\ell,q')}]_\ell$ is finite for $(q, q') \notin \mathcal{S}$ and since the sets $[L_{(k,q)}]_k \cap [L_{(\ell,q')}]_\ell$ cover $\mathbb{N}$ there is some natural number M such that every natural number $n \geq M$ is in $[L_{(k,q)}]_k \cap [L_{(\ell,q')}]_\ell$ for some $(q, q') \in \mathcal{S}$.

By Dirichlet's theorem, for each $\epsilon > 0$, there exist $m, n \in \mathbb{N}$ such that $|k^n - \ell^m| \leq \epsilon \min(k^n, \ell^m)$. Take $\epsilon = \frac{1}{6N}$ where

$$N = \max\{x_{(q,q')} \colon (q, q') \in \mathcal{S}\} + 1.$$

Now, without loss of generality, we may assume $k^n > \ell^m$. So we have

$$|k^n - \ell^m| \leq \frac{1}{6N}\ell^m. \tag{2.14}$$

Then for each pair $(x, y) = (x_{(q,q')}, y_{(q,q')})$ we have chosen above, since $x_{(q,q')} \neq y_{(q,q')}$ and $k^n \neq \ell^m$, we have that

$$p_{(q,q')} := (x_{(q,q')} - y_{(q,q')})(k^n - \ell^m)$$

is not zero, and in fact it is strictly greater than zero by our assumptions. Then by Inequality 2.14, we have $0 < p_{(q,q')} \leq \frac{\ell^m}{6}$ for all $q' \in Q_\infty$. We show that for each $(q, q') \in \mathcal{S}$, the sequence $\{a(n)\}_n$ has local period $p_{(q,q')}$ on I_c for every $c \in [L_{k,q}]_k \cap [L_{\ell,q'}]_\ell$, where

$$I_c := B[c\ell^m; \frac{2}{3}\ell^m].$$

That is, we will show that $a(c\ell^m+z)=a(c\ell^m+z+p_{(q,q')})$ whenever $z, z+p_{(q,q')} \in B[0;\frac{2}{3}\ell^m]$. Pick $z, z+p_{(q,q')} \in B[0;\frac{2}{3}\ell^m]$. Note that

$$|z-y_{(q,q')}(k^n-\ell^m)| \leq |z|+|y_{(q,q')}(k^n-\ell^m)| \leq \frac{2}{3}\ell^m+\frac{1}{6}\ell^m=\frac{5}{6}\ell^m<\ell^m<k^n.$$

So

$$z-y_{(q,q')}(k^n-\ell^m) \in B(0;k^n) \subseteq [D_k^n]_k.$$

Now, for $(q,q') \in \mathcal{S}$ and $c \in [L_{k,q}]_k \cap [L_{\ell,q'}]_\ell$, since $z \in [D_\ell^m]_\ell$, we have

$$\begin{aligned}
a(c\ell^m+z) &= a(y_{(q,q')}\ell^m+z) \text{ by Equation 2.13 since both } c \text{ and } y_{(q,q')} \text{ are in } [L_{\ell,q'}]_\ell\\
&= a(y_{(q,q')}k^n+z-y_{(q,q')}(k^n-\ell^m))\\
&= a(x_{(q,q')}k^n+z-y_{(q,q')}(k^n-\ell^m)) \text{ by Equation 2.12 since}\\
&\qquad\qquad x_{(q,q')}, y_{(q,q')} \in [L_{k,q}]_k \cap [L_{\ell,q'}]_\ell\\
&= a(x_{(q,q')}\ell^m+z+p_{(q,q')}) \text{ since } p_{(q,q')}=(x_{(q,q')}-y_{(q,q')})(k^n-\ell^m)\\
&= a(c\ell^m+z+p_{(q,q')}) \text{ by Equation 2.13 since both } c \text{ and } x \text{ are in } [L_{\ell,q'}]_\ell.
\end{aligned}$$

Therefore, we have shown that for each $(q,q') \in \mathcal{S}$, the sequence $\{a(n)\}_n$ has local period $p_{(q,q')}$ on I_c for every $c \in [L_{k,q}]_k \cap [L_{\ell,q'}]_\ell$, where $I_c := B[c\ell^m;\frac{2}{3}\ell^m]$. Earlier we saw that there exists an integer M such that all natural numbers $j \geq M$ have the property that j is in $[L_{k,q}]_k \cap [L_{\ell,q'}]_\ell$ for some $(q,q') \in \mathcal{S}$.

Then from the above, for each $j \geq M$ there is some $p_j \leq \frac{1}{6}\ell^m$ that is a local period of $\{a(n)\}_n$ on I_j. We show that $\{a(n)\}_n$ has local period p_M on

$$\bigcup_{M \leq j \leq s} I_j$$

for all $s \geq M$ by induction on s. If $s=M$, then $\{a(n)\}_n$ has local period p_M on $\bigcup\limits_{M \leq j \leq s} I_j = I_M$ by construction. Now suppose $\{a(n)\}_n$ has local period p_M on $\bigcup\limits_{M \leq j < s} I_j$ and has local period p_s on I_s. Now we use Lemma 53 as follows. We show that

$$\left(\bigcup_{M \leq j < s} I_j\right) \cap I_s$$

has cardinality greater than or equal to p_M+p_s. Since $\left(\bigcup\limits_{M \leq j < s} I_j\right) \cap I_s = B[(s-\dfrac{1}{2})\ell^m); \dfrac{1}{6}\ell^m]$ and $B[(s-\frac{1}{2})\ell^m); \frac{1}{6}\ell^m]$ has cardinality at least $\frac{\ell^m}{3} \geq p_M+p_s$, we have that $\{a(n)\}_n$ has local period p_M on $\bigcup\limits_{M \leq j \leq s} I_j$, by Lemma 53. So $\{a(n)\}_n$ has local period p_M on $\bigcup\limits_{M \leq j} I_j$, and since this set contains all sufficiently large natural numbers, this gives that $\{a(n)\}_n$ is ultimately periodic. □

We conclude this section by looking at one nice application of Cobham's theorem.

Example 58. Let p be prime and consider the set $S = \{1, p, p^2, p^3, \dots\}$. We have seen that this set is p-automatic and that, moreover, by Proposition 18 it is p^m-automatic for each $m \geq 1$. Also the sequence $\chi_S(n)$ is not ultimately periodic since it has arbitrarily long runs of zeros without being eventually zero. So for a number k that is not a power of p, i.e. $k \neq p^m$ for any $m \geq 1$, S cannot be a k-automatic set by Cobham's theorem.

Chapter 3

Number Theoretic Preliminaries

In this chapter, we give the number theoretic background necessary for proving part (b) of Theorem 3 and also some background needed for the strong version of Cobham's theorem proved in Chapter 4. For the characterization of sparse series valuations and Artin-Schreier extensions are involved. For the strong version of Cobham's theorem that we will give, we require the theory of S-unit equations and Schlickewei's theorem [40].

3.1 Ramification and Artin-Schreier Extensions

We first introduce places and valuations. Let $\Bbbk$ be a field and let K be a field extension of $\Bbbk$. A *valuation* of K is a map $\nu : K \to \Gamma \cup \{\infty\}$, where Γ is a totally ordered abelian group, such that the following conditions are met:

(i) $\nu(a) = \infty$ if and only if $a = 0$;

(ii) $\nu(ab) = \nu(a) + \nu(b)$;

(iii) $\nu(a + b) \geq \min(\nu(a), \nu(b))$, with equality whenever $\nu(a) \neq \nu(b)$.

We say that a valuation is *trivial* if it is zero on all nonzero elements of the field. We define the *rank* of a valuation to be the rank of the abelian group Γ; i.e., the dimension of $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space, and we say that a valuation is *discrete* if its value group Γ is $\mathbb{Z}$.

Given a valuation, we have a *valuation ring* $\mathcal{O}_\nu \subseteq K$ consisting of elements with nonnegative valuation. Then $\mathcal{O}_\nu$ is a local ring with a unique maximal ideal, which we denote $\mathcal{M}_\nu$, given by the collection of elements with strictly positive valuation. The *residue field* of a valuation is defined to be $\mathcal{O}_\nu/\mathcal{M}_\nu$. We say that two valuations of K are *equivalent* if they have the same valuation ring and we call an equivalence class of valuations of K a *place* of K. We will often use an equivalence class representative to represent a place. We will generally deal with discrete valuations ν, in which case the valuation ring $\mathcal{O}_\nu$ is a principal ideal domain and a generator for the maximal ideal $\mathcal{M}_\nu$ is called a *uniformizing parameter*.

In the case where $\Bbbk$ is an algebraically closed field and K is a finitely generated extension of $\Bbbk$ of transcendence degree one, there is a smooth projective curve X over $\Bbbk$ such that K is the function field of X. Then if we look at non-trivial places of K with trivial restriction to $\Bbbk$, these are parametrized by the closed points of X as follows. Given $x \in X$, we can define a valuation $\nu_x : K \to \mathbb{Z} \cup \{\infty\}$ by taking $\nu_x(f)$ to be the order of vanishing of the function f at the point x (see [48, Ch. VI, §17]).

In the case we are interested in, $\Bbbk$ will be the algebraic closure of a finite field and in this case, every valuation of K has trivial restriction to $\Bbbk$. From the above, we then have that the non-trivial places of the field $\bar{\mathbb{F}}_p(t)$ are parametrized by the projective line over $\bar{\mathbb{F}}_p$.

We now use places to define ramification.

Definition 59. Given a finite extension of fields $L \supseteq K$, we say L is *unramified* at a place ν of K if the value group of every extension of ν to L is the same as the value group of ν.

In our case, we generally deal with discrete valuations, and a place ν of K has finitely many extensions $\nu_1, \ldots, \nu_s$ to L. Then for each $i \in \{1, \ldots, s\}$ we have a discrete valuation ring $\mathcal{O}_{\nu_i} \subseteq L$ consisting of elements in L with nonnegative valuation with ν_i, and similarly we have a discrete valuation ring $\mathcal{O}_\nu \subseteq K$. Then these are local rings whose maximal ideals are principal and we have $\mathcal{O}_\nu \subseteq \mathcal{O}_{\nu_i}$. Then if π is a generator for the maximal ideal of $\mathcal{O}_\nu$ and if L is unramified at ν then π will also generate the maximal ideal of $\mathcal{O}_{\nu_i}$ for $i = 1, \ldots, s$. Furthermore, we will often work with places that are parametrized by points in $\mathbb{P}^1$ and so we will often identify places with the corresponding points in projective space.

In our setting, the fields K and K' we work with will have the property that the compositum of two finite extensions of K inside K' that are unramified at some place ν of K is again unramified at ν (see Serre [42, Chapter III] for further details).

The final algebraic ingredients we will use in proving Theorem 3 are the notion of Artin-Schreier extensions, which are degree-p Galois extensions of fields of positive characteristic p, and the notion of integrality. We first quickly recall the relevant definitions for integral elements.

Given integral domains $S \subseteq T$, we say that $u \in T$ is *integral* over S if there is a monic polynomial $f(x) \in S[x]$ with $f(u) = 0$. The set of elements of T that are integral over S forms a ring and is called the *integral closure* of S in T. We say that S is *integrally closed* if S is integrally closed in its field of fractions. Finally, we recall the notion of Artin-Schreier extensions.

For the proof of the following theorem, see Lang [33, VI.6.4].

Theorem 60 (Artin-Schreier Theorem)**.** *Let p be prime, let $\Bbbk$ be a field of characteristic p, and let K be a Galois extension of $\Bbbk$ of degree p.*

(1) There exists $\alpha \in K$ such that $K = \Bbbk(\alpha)$ and α is the root of a polynomial $X^p - X - a$ for some $a \in \Bbbk$.

(2) Conversely, given $a \in \Bbbk$, the polynomial $f(X) = X^p - X - a$ either has one root in $\Bbbk$, in which case all its roots are in $\Bbbk$, or it is irreducible. In this latter case, if α is a root then $\Bbbk(\alpha)$ is cyclic Galois extension of $\Bbbk$ of degree p.

The Artin-Schreier theorem provides an inductive means of describing Galois extensions of size a power of p.

Remark 61. *Let $\Bbbk$ be a field of characteristic $p > 0$ and let K be a Galois extension of $\Bbbk$ of degree p^m for some $m \geq 0$. Then there exists a chain of fields $\Bbbk = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$ with each K_i a Galois extension of $\Bbbk$ and such that K_{i+1} is an Artin-Schreier extension of K_i for $i = 0, \ldots, m-1$.*

Proof. This follows immediately from the fundamental theory of Galois theory combined with the fact that a group P of order p^m is nilpotent and hence has a chain of subgroups

$$P = P_0 \trianglerighteq P_1 \trianglerighteq \cdots \trianglerighteq P_m = \{1\}$$

with each P_i normal in P and $|P_i| = p^{m-i}$ for $i = 1, \ldots, m$. □

3.2 S-unit equations

In this brief section we give an overview of the theory of S-unit equations. Specifically, we require a quantitative version of a result due to Evertse, Schlickewei and Schmidt (see [22, Theorem 1.1] and also [21, Theorem 6.1.3]).

Definition 62. *Let L be a field and let $a_1, \ldots, a_m \in L$ be nonzero elements of L. Then a solution $y_1, \ldots, y_m \in L$ to the equation*

$$a_1 y_1 + \cdots + a_m y_m = 1$$

is called non-degenerate *if the left side has no non-trivial vanishing subsums i.e. if* $\sum_{i \in I} a_i y_i \neq 0$ *for each non-empty subset I of $\{1, \ldots, m\}$.*

Theorem 63. *Let L be a field of characteristic zero, let $a_1, \ldots, a_m$ be nonzero elements of L, and let $H \subset (L^\times)^m$ be a finitely generated multiplicative group. Then there are only finitely many non-degenerate solutions $(y_1, \ldots, y_m) \in H$ to the equation $a_1 y_1 + \cdots + a_m y_m = 1$.*

Theorem 6.1.3 in [21] is only stated for $m \geq 2$, but the case $m = 1$ is immediate.

We will require a quantitative version of the S-unit theorem due to Schlickewei [40].

To describe this result, we require some background. We let K be a number field that is Galois over $\mathbb{Q}$. Recall that places of K are simply equivalence classes of valuations of K. We recall that the p-adic valuation on $\mathbb{Q}$ gives rise to an absolute value. Then valuations are equivalent when the corresponding absolute values induce the same topology on the field. In fact, it is often more convenient to work with absolute values as proxies for places, and then one sees that there are two types of places of a number field: finite places, which correspond to absolute values whose restriction to $\mathbb{Q}$ is equivalent to the p-adic absolute value for some prime p; and infinite places, which correspond to absolute values whose restriction to $\mathbb{Q}$ is equivalent to the ordinary Euclidean absolute value. While a number field K has infinitely many finite places, it only has finitely many infinite places; moreover, the number of infinite places is at most the degree of the number field over $\mathbb{Q}$.

We now let S be a finite set of places of K that includes all the infinite places. Then we have a ring $\mathcal{O}_{K,S}$ consisting of elements $x \in K$ for which $|x|_v \leq 1$ for all $v \notin S$. We let $U_{K,S}$ denote the units group of $\mathcal{O}_{K,S}$. With this notation in place, we have the following result due to Schlickewei [40].

Theorem 64. *Let $n \geq 1$, let K be a number field that is Galois over $\mathbb{Q}$, and let S be a finite set of places of K that includes all the infinite places. If $a_1, \ldots, a_n \in K$, then the number of non-degenerate solutions to the equation $a_1 x_1 + \cdots + a_n x_n = 1$ with $(x_1, \ldots, x_n) \in U_{K,S}^n$ is bounded above by $(4|S|D)^{2^{36n|D|}|S|^6}$, where $D = [K : \mathbb{Q}]$.*

Chapter 4

A Strong Version of Cobham

In this chapter we prove a strong version of Cobham's theorem for sparse sets. In particular, we prove a quantitative version of Theorem 1 given in the Introduction.

4.1 Intersections of sparse sets

We now consider the intersection of a sparse k-automatic set and a sparse ℓ-automatic set of natural numbers and show that one can bound the size of the intersection in terms of the number of states of the DFAOs that generate the sets. We begin with a basic estimate.

Lemma 65. *Let r, k, q be integers with $r \geq 1$, $k \geq 2$ and $q > r$. Then*

$$rk(k^{q-r} + \cdots + k + 1) + r \leq (k^q + k^{q-1} + \cdots + 1).$$

Proof. We have $(q-r)rk(k^{q-r} + \cdots + k + 1) + r \leq (q-r)r((k^{q-r+1} + k^{q-r} + \cdots + k) + 1)$. Now since $k \geq 2$, we have $k^{r-1} \geq 2^{r-1} \geq r$ for all $r \geq 1$. Hence

$$r(k^{q-r+1} + k^{q-r} + \cdots + 1) \leq k^{r-1}(k^{q-r+1} + k^{q-r} + \cdots + 1) \leq k^q + k^{q-1} + \cdots + 1,$$

and so we get the desired result. □

Proposition 66. *Let $k \geq 2$ and $\Gamma = (Q, \Sigma_k, \delta, q_0, F)$ be a deterministic finite-state automaton accepting a sparse non-trivial language $\mathcal{L}$. Then $\mathcal{L}$ is a finite (possibly empty) union of at most $|Q|!(k^{|Q|} + k^{|Q|-1} + \cdots + 1)$ sets of the form*

$$\{v_0 w_1^* v_1 w_2^* \cdots v_{s-1} w_s^* v_s\}$$

with $w_1, \ldots, w_s, v_1, \ldots, v_s$ words in Σ_k^* in which the w_i are non-empty but the v_i may be empty and with $|w_1| + \cdots + |w_s| \leq |Q|$ and $|v_0| + \cdots + |v_s| \leq k|Q|$.

Proof. Suppose towards a contradiction that this is not the case and pick $(Q, \Sigma_k, \delta, q_0, F)$ for which the conclusion to the statement of the proposition does not hold with $|Q|$ minimal. We put a transitive binary relation $\prec$ on Q by declaring that $q \prec q'$ for $q, q' \in Q$ if there is a word $w \in \Sigma_k^*$ such that $\delta(q, w) = q'$. We then declare that two states q, q' are equivalent if $q \prec q'$ and $q' \prec q$. Then this relation is reflexive as $\delta(q, \epsilon) = q$ and so $q \prec q$ and it is symmetric and transitive by construction. We let $[q]$ denote the equivalence class of q. Then $\prec$ induces a partial order on the equivalence classes. We let r denote the size of the equivalence class $[q_0]$. Since $\mathcal{L}$ is non-empty, there is at least one path from q_0 to an accepting state. In particular, by Proposition 22, we have that there is at most one cycle based at q_0 and since it passes through all states in $[q_0]$, this cycle, if it exists, is some word w_1 of length r. We note that if $r \geq 2$ then there must be a cycle based at q_0, but if $r = 1$ it is possible that $\delta(q_0, w) = q_0$ if and only if $w = \epsilon$. We now consider two cases corresponding to these possibilities. The simpler case is when $\delta(q_0, w) = q_0$ only if $w = \epsilon$. In this case, $[q_0] = q_0$ and for each $x \in \Sigma_k$, we let $\mathcal{L}_x$ denote the set of all words $w \in \Sigma_k^*$ whose first letter is x and for which $w \in \mathcal{L}$. Then $\delta(q_0, u_x) \in Q \setminus \{q_0\}$ for every $u_x \in \mathcal{L}_x$. Then since q_0 is only equivalent to itself, we see that $\mathcal{L}_x = x\mathcal{E}_x$, where $\mathcal{E}_x$ is the regular language accepted by the automaton $\Gamma_x := (Q \setminus \{q_0\}, \Sigma_k, \delta, \delta(q_0, x), F \setminus \{q_0\})$.

Then by minimality of $|Q|$, we have that $\mathcal{E}_x$ is a union of at most $(|Q| - 1)!(k^{|Q|-1} + \cdots + 1)$ sets of the form

$$\{v_0 w_1^* v_1 w_2^* \cdots v_{s-1} w_s^* v_s\}$$

with $w_1, \ldots, w_s, v_1, \ldots, v_s$ words in Σ_k^* in which the w_i are non-empty but the v_i may be empty and with $|w_1| + \cdots + |w_s| \leq |Q| - 1$ and $|v_0| + \cdots + |v_s| \leq k(|Q| - 1)$. Then $\mathcal{L}_x$ is a union of at most $(|Q| - 1)!(k^{|Q|-1} + \cdots + 1)$ sets of the form

$$\{(xv_0) w_1^* \cdots v_{s-1} w_s^* v_s\}$$

with $w_1, \ldots, w_s, v_0, \ldots, v_s$ words in Σ_k^* in which the w_i are non-empty but the v_i may be empty and with $|w_1| + \cdots + |w_s| \leq |Q|$ and $|xv_0| + \cdots + |v_s| \leq k|Q|$, since $k \geq 1$. Then since $\mathcal{L}$ is the union of $\mathcal{L}_x$ for $x \in \Sigma_k$ we see that $\mathcal{L}$ is a union of at most $(|Q| - 1)!(k^{|Q|} + k^{|Q|-1} + \cdots + k)$ sets of the form

$$\{v_0 w_1^* v_1 w_2^* \cdots v_{s-1} w_s^* v_s\}$$

with $w_1, \ldots, w_s, v_1, \ldots, v_s$ words in Σ_k^* in which the w_i are non-empty but the v_i may be empty and with $|w_1| + \cdots + |w_s| \leq |Q|$ and $|v_0| + \cdots + |v_s| \leq k|Q|$. Thus we obtain the result in this case.

We next consider the case when there is a unique cycle w_1 of length $r \geq 1$ based at q_0. In particular, $\#[q_0] = r$. Then in this case we can write $\mathcal{L} = \mathcal{L}_0 \cup \mathcal{L}_1$, where $\mathcal{L}_0$ is the set of words w in $\mathcal{L}$ for which $\delta(q_0, w) \in [q_0]$ and $\mathcal{L}_1$ is the set of words $w \in \mathcal{L}$ for which $\delta(q_0, w) \notin [q_0]$. By construction every word in $\mathcal{L}_0$ is of the form $w_1^* v$ where v is a proper prefix of w_1. In particular, $\mathcal{L}_0$ is a union of at most r sets of the desired form. We next consider $\mathcal{L}_1$. If $w \in \mathcal{L}_1$ then w can be written as uxv with $\delta(q_0, u) \in [q_0]$, $\delta(q_0, ux) \notin [q_0]$. Then we may write $\mathcal{L}_1$ as a union of $|Q| - r$ sublanguages $\mathcal{L}_{1,q}$ for each $q \in Q \setminus [q_0]$, where $\mathcal{L}_1$ is the set of words in $\mathcal{L}$ of the form uxv with $\delta(q_0, u) \in [q_0]$, $\delta(q_0, ux) = q$. We have a machine $\Gamma_q = (Q \setminus [q_0], \Sigma_k, \delta, q, F \setminus [q_0])$, which accepts a sparse regular language $\mathcal{E}_q$. Then $\mathcal{L}_{1,q}$ is a finite union of languages of the form $w_1^* zx\mathcal{E}_q$ where z is a proper prefix of w_1, $x \in \Sigma_k$ and $\delta(q_0, zx) = q$. In particular, by minimality of $|Q|$, each $\mathcal{E}_q$ is a finite union of at most $(|Q| - r)!(k^{|Q|-r} + \cdots + 1)$ sets of the form

$$\{v_1 w_2^* v_2 w_3^* \cdots v_{s-1} w_s^* v_s\}$$

with $|w_2| + \cdots + |w_s| \leq |Q| - r$ and $|v_1| + \cdots + |v_s| \leq k(|Q| - r)$. Then since w has at most r proper prefixes and since there are at most k choices for x, we see that $\mathcal{L}_{1,q}$ is a union of at most $(rk)(|Q| - r)!(k^{|Q|-r} + \cdots + k + 1)$ sets of the form

$$\{w_1^*(zxv_1) w_2^* v_2 w_3^* \cdots v_{s-1} w_s^* v_s\}$$

with $|w_1| + \cdots + |w_s| \leq |Q|$ and $|zxv_1| + \cdots + |v_s| \leq k(|Q| - r) + r \leq k|Q|$. Thus $\mathcal{L}$ is a union of at most $(|Q| - r)rk(|Q| - r)!(k^{|Q|-r} + \cdots + k + 1) + r$ sets of the desired form, where the contribution of r comes from considering our decomposition of $\mathcal{L}_0$ and the $|Q| - r$ factor comes from considering the languages $\mathcal{L}_{1,q}$ for $q \in Q \setminus [q_0]$. Notice that $(|Q| - r)rk(|Q| - r)!(k^{|Q|-r} + \cdots + k + 1) + r \leq |Q|!(k^{|Q|} + \cdots + k + 1)$ by Lemma 65. □

For the remainder of the section, we make use of a Theorem 64, due to Schlickewei [40].

For us, we will apply Theorem 64, taking $K = \mathbb{Q}$ and S to be the set of places corresponding to prime divisors of numbers k and ℓ along with the infinite place.

Lemma 67. *Let k and ℓ be multiplicatively independent integers and let $n, m \geq 1$ be integers and let $a_1, \ldots, a_n, b_1, \ldots, b_m$ be nonzero rational numbers. Then there are at most*

$$(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6 \cdot 2^{36(n+m-1)}}$$

non-degenerate solutions to the equation

$$a_1 X_1 + \cdots + a_n X_n + b_1 Y_1 + \cdots + b_m Y_m = 0$$

in which each X_i is a power of k, each Y_i is a power of ℓ.

Proof. We take S to be the places corresponding to the infinite place of $\mathbb{Q}$ along with the places corresponding to the prime divisors of k and ℓ. Then since each prime factor of k and ℓ is at least two, we have $|S| \leq \log_2(k) + \log_2(\ell) + 1$. Further, by construction, k and ℓ are in the units group of $\mathcal{O}_{\mathbb{Q},S}$. Now a non-degenerate solution to the equation

$$a_1X_1 + \cdots + a_nX_n + b_1Y_1 + \cdots + b_mY_m = 0$$

with each X_i a power of k and each Y_j a power of ℓ gives rise to a non-degenerate solution to the equation

$$(-a_1/b_m)Z_1 + \cdots + (-a_n/b_m)Z_n + (-b_1/b_m)Z_{n+1} + \cdots + (-b_{m-1}/b_m)Z_{n+m-1} = 1$$

with $Z_i = X_i/Y_i$ for $i \leq n$ and $Z_i = Y_{i-n}/Y_m$ for $n+1 \leq i < n+m$. Since the Z_i are in the units group of $\mathcal{O}_{\mathbb{Q},S}$, Theorem 64 gives that there are at most

$$(4|S|)^{2^{36(n+m-1)}|S|^6}$$

non-degenerate solutions with $Z_1, \ldots, Z_{n+m-1}$ in $\mathcal{O}_{\mathbb{Q},S}$. Now the final remark is that we can uniquely recover the original X_i's and Y_i's from $Z_1, \ldots, Z_{n+m}$. To see this, observe that for $i = 1, \ldots, n$ we must have $Z_i = k^a/\ell^b$ for some integers a and b. Since k and ℓ are multiplicatively independent, a and b are uniquely determined and so $X_i = k^a$ and $Y_m = \ell^b$. Thus we can recover $X_1, \ldots, X_n$ and Y_m from the Z_j. But once we know $Y_m = \ell^b$, since $Y_j = Z_{n+j}Y_m$ for $j = 1, \ldots, m-1$, we see that we can recover the Y_j's from $Z_1, \ldots, Z_{n+m-1}$. Using the fact that $|S| \leq \log_2(2k\ell)$ gives the desired result. □

Lemma 68. *Let k and ℓ be multiplicatively independent integers and let $n, m \geq 1$ be integers and let $a_1, \ldots, a_n, b_1, \ldots, b_m$ be nonzero rational numbers. Then there are at most*

$$(n+m)^{n+m+1}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6 \cdot 2^{36(n+m-1)}}$$

solutions to the equation

$$a_1X_1 + \cdots + a_nX_n + b_1Y_1 + \cdots + b_mY_m = 0$$

in which each X_i is a power of k, each Y_i is a power of ℓ, and no non-trivial subsum of either $a_1X_1 + \cdots + a_nX_n$ or $b_1Y_1 + \cdots + b_mY_m$ vanishes.

Proof. For each solution to

$$a_1X_1 + \cdots + a_nX_n + b_1Y_1 + \cdots + b_mY_m = 0$$

such that no subsum of either $a_1X_1 + \cdots + a_nX_n$ or $b_1Y_1 + \cdots + b_mY_m$ vanishes, we can associate a set partition π of the set $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ into disjoint non-empty subsets $U_1, \ldots, U_r$ such that the subsum corresponding to the variables in each U_i vanishes and is non-degenerate. Then by Lemma 67, for $i = 1, \ldots, r$, there are at most $(4A)^{2^{36(|U_i|-1)}A^6}$ non-degenerate solutions to the subsum

$$\sum_{X_j \in U_i} a_jX_j + \sum_{Y_j \in U_i} b_jY_j = 0$$

with each X_j a power of k and each Y_j a power of ℓ. Thus for the set partition π we have at most

$$\prod_{i=1}^{r} (4A)^{2^{36|U_i|)}A^6} = (4A)^{A^6 \cdot \sum_{i=1}^{r} 2^{36|U_i|}}$$

solutions. Using the inequality $2^{x_1+x_2+\cdots+x_r} \geq \sum_{i=1}^{r} 2^{x_i}$ for $x_1, \ldots, x_r$ positive integers, we see that corresponding to the set partition π we get at most

$$(4A)^{A^6 \cdot 2^{36(n+m-1)}}$$

solutions. Finally, observe that there is a natural injection from the collection of set partitions of $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ of size r into maps f from $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ to $\{1, 2, \ldots, r\}$, by imposing some ordering on the subsets in our set partition and then declaring that $f(X_i) = j$ if X_i is in the j-th set of our partition and similarly, declaring that $f(Y_i) = j$ if Y_i is in the j-th set of our partition. It follows that there are at most r^{n+m} set partitions of $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$ of size r and since r can range from 1 to $n + m$, we then get that there are at most $(n + m)^{n+m+1}$ set partitions of $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$. Since we get at most

$$(4A)^{A^6 \cdot 2^{36(n+m-1)}}$$

solutions of the desired form corresponding to each set partition of $\{X_1, \ldots, X_n, Y_1, \ldots, Y_m\}$, and since there are at most $(n+m)^{n+m+1}$ set partitions, we get the desired upper bound. □

Proposition 69. *Let k and ℓ be multiplicatively independent positive integers and let X be a sparse k-automatic subset of $\mathbb{N}$ of the form*

$$\{[v_0w_1^*v_1w_2^* \cdots v_sw_s^*v_{s+1}]_k\}$$

and let Y be a sparse ℓ-automatic set of the form

$$\{[u_0y_1^*u_1y_2^* \cdots u_ty_t^*u_{t+1}]_\ell\}.$$

Then

$$\#X \cap Y \leq (s + t + 2)^{s+t+3}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6 \cdot 2^{36(s+t+1)}}.$$

Proof. By Lemma 33 we have that X is of the form

$$\left\{c_0 + c_1 k^{\delta_s n_s} + c_2 k^{\delta_s n_s + \delta_{s-1} n_{s-1}} \cdots + c_s k^{\delta_s n_s + \cdots + \delta_1 n_1} \colon n_1, \ldots, n_s \geq 0\right\},$$

where $c_0, \ldots, c_s$ are rational numbers. Similarly, Y is of the form

$$\left\{d_0 + d_1 \ell^{\delta'_t m_t} + d_2 \ell^{\delta'_t m_s + \delta'_{t-1} m_{t-1}} \cdots + d_t \ell^{\delta'_t m_t + \cdots + \delta'_1 m_1} \colon m_1, \ldots, m_t \geq 0\right\},$$

where $d_0, \ldots, d_t$ are rational numbers.

Then an element in $X \cap Y$ corresponds to a solution to the equation

$$X_0 + \cdots + X_t + X_{t+1} + \cdots + X_{t+s+1} = 0,$$

where $X_0 = d_0, X_1 = d_1 \ell^{\delta'_t m_t}, \ldots, X_t = d_t \ell^{\delta'_t m_t + \cdots + \delta'_1 m_1}$ and $X_{t+1} = -c_0$, $\ldots$, $X_{t+s+1} = -c_s k^{\delta_s n_s + \cdots + \delta_1 n_1}$. Moreover, the element in the intersection in this case is given by

$$A := X_0 + \cdots + X_t = -(X_{t+1} + \cdots + X_{t+s+1}).$$

Observe that $A = X_0 + \cdots + X_t$ is strictly positive and since we are only concerned about the quantity A in determining $X \cap Y$, after removing a maximal vanishing subsum we may assume that no non-trivial subsum of the terms involving powers of ℓ vanishes and that there are at most $t + 1$ such terms. Similarly, we may remove a maximal vanishing subsum from $X_{t+1} + \cdots + X_{t+s+1}$. Then by Lemma 68, taking n to be the number of terms from our first sum, we have $n \leq t + 1$; similarly, we can take m to be the number of terms from our second subsum and we have $m \leq s + 1$. We then see there are at most

$$(s + t + 2)^{s+t+3}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6 \cdot 2^{36(s+t+1)}}$$

elements in $X \cap Y$. □

We are now ready to put everything together and prove the strong version of Cobham's theorem.

Theorem 70. *(Strong Cobham theorem for sparse sets) Let k and ℓ be multiplicatively independent positive integers and let $\Gamma = (Q, \Sigma_k, \delta, q_0, F)$ and $\Gamma' = (Q', \Sigma_\ell, \delta', q'_0, F')$ be a deterministic finite-state automata accepting sparse languages $\mathcal{L} \subseteq \Sigma_k^*$ and $\mathcal{L}' \subseteq \Sigma_\ell^*$. Then if $X = [\mathcal{L}]_k$ and $Y = [\mathcal{L}']_\ell$ then $X \cap Y$ is finite and there are at most $A \cdot B$ elements in the intersection, where*

$$A = |Q|!|Q'|!(k^{|Q|} + k^{|Q|-1} + \cdots + 1)(\ell^{|Q'|} + \ell^{|Q'|-1} + \cdots + 1)$$

and

$$B = (|Q| + |Q'| + 2)^{|Q|+|Q'|+3}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6 \cdot 2^{36(|Q|+|Q'|+1)}}.$$

Proof. By Proposition 69, X is the union of at most $|Q|!(k^{|Q|}+k^{|Q|-1}+\cdots+1)$ sets of the form

$$\{v_0w_1^*v_1w_2^*\cdots v_{s-1}w_s^*v_s\}$$

with $w_1,\ldots,w_s,v_0,\ldots,v_s$ words in Σ_k^* in which the w_i are non-empty but the v_i may be empty and with $|w_1|+\cdots+|w_s|\le|Q|$ and $|v_0|+\cdots+|v_s|\le k|Q|$. In particular, $s\le|Q|$ for each such set. Similarly, Y is the union of at most $|Q'|!(\ell^{|Q'|}+\ell^{|Q'|-1}+\cdots+1)$ sets of the form

$$\{u_0y_1^*u_1y_2^*\cdots u_{t-1}y_t^*u_{t+1}\}$$

with $u_0,\ldots,u_{t+1},y_1,\ldots,y_t$ words in Σ_ℓ^* in which the y_i are non-empty but the u_i may be empty and with $|y_1|+\cdots+|y_t|\le|Q'|$ and $|u_0|+\cdots+|u_t|\le\ell|Q'|$. In particular, $t\le|Q'|$ for each such set. Then by Proposition 69, each pair of sets of the above form has cardinality at most

$$(s+t+2)^{s+t+3}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6\cdot 2^{36(s+t+1)}}$$

in the intersection. In particular, since $s\le|Q|$ and $t\le|Q'|$ and since we have at most

$$|Q|!|Q'|!(k^{|Q|}+k^{|Q|-1}+\cdots+1)(\ell^{|Q'|}+\ell^{|Q'|-1}+\cdots+1)$$

pairs, we see that there are at most $N=N(k,\ell,|Q|,|Q'|)$ elements in the intersection of X and Y, where N is the product of

$$|Q|!|Q'|!(k^{|Q|}+k^{|Q|-1}+\cdots+1)(\ell^{|Q'|}+\ell^{|Q'|-1}+\cdots+1)$$

and

$$(|Q|+|Q'|+2)^{|Q|+|Q'|+3}(4(\log_2(2k\ell)))^{(\log_2(2k\ell))^6\cdot 2^{36(|Q|+|Q'|+1)}}.$$

Hence the result follows. □

We note that some dependence on k and ℓ is necessary as well as dependence on the number of states. For example, one can write down a k-DFAO with n states that accepts all numbers less than k^{n-2}; similarly, one can write down an ℓ-DFAO with m states that accepts all natural numbers less than ℓ^{m-2}. In particular, the intersection of the two sets generated by these automata will have intersection of size $\min(k^{n-2},\ell^{m-2})$, and so although this is far off from the upper bounds we obtain, it nevertheless shows that one cannot completely eliminate some dependence on the number of states in our result.

4.2 A general intersection question

We now consider the general question of the intersection of a sparse automatic set with a zero density automatic set.

The following result is due to Bell [9, Prop. 2.1].

Proposition 71. *Let $k \geq 2$ be a natural number, let $h : \mathbb{N} \to \mathbb{Q}_{\geq 0}$ be a k-automatic sequence, and let $s(n) = \sum_{j<n} h(j)$. Then there exist $\beta \in (0, k)$, $C > 0$, $a \geq 1$, and rational numbers c_j for $j \in \{0, 1, \ldots, a-1\}$ such that*

$$|s(k^{an+j}) - c_j k^{an+j}| < C\beta^{an}$$

for every $n \geq 0$. Moreover, a and the rational numbers $c_0, \ldots, c_{a-1}$ are recursively computable and β can be effectively determined.

As a consequence of this, we can prove that either a k-automatic set S has positive lower density (i.e., $\liminf \pi_S(x)/x > 0$) or there is some positive $\epsilon > 0$ such that $\pi_S(x) = \mathrm{o}(x^{1-\epsilon})$. Moreover, we can find a lower bound for ϵ in terms of the size of the k-kernel for the automatic sequence corresponding to S.

Theorem 72. *Let $k \geq 2$ be a natural number and let S be a k-automatic subset of the natural numbers associated with a k-automatic sequence whose k-kernel has size $d \geq 2$. Then either S has positive lower density or*

$$\pi_S(x) = \mathrm{o}(x^{1-\epsilon})$$

with $\epsilon = 1 - 1/(2k)^{d-1} + 1/2(2k)^{2(d-1)}$.

Proof. The proof of Proposition 71 [9] shows that either S has positive lower density or $\pi_S(k^n) = \mathrm{o}(\beta^n)$ for some $\beta \in (0, k)$ such that β is bigger in modulus than all eigenvalues of a $d \times d$ matrix B with nonnegative integer entries whose eigenvalues all lie in the disc $\{z \colon |z| < k\}$. We henceforth assume that we are in the second case. In particular, if $\alpha_1, \ldots, \alpha_d$ are the roots (with multiplicity) of the characteristic polynomial, $P(x)$, of B then $P(k) = (k - \alpha_1) \cdots (k - \alpha_d)$ is a nonzero integer. By the Perron-Frobenius theorem (see e.g. [2], Theorem 8.3.7), after relabelling, we may assume that α_1 is real and positive and that $|\alpha_i| \leq \alpha_1$ for $i = 1, 2, \ldots, d$. Then since each α_i is less than k in modulus, we have

$$\begin{aligned} 1 &\leq |P(k)| \\ &= |k - \alpha_1| \prod_{i=2}^{d} |k - \alpha_i| \\ &< |k - \alpha_1|(2k)^{d-1}. \end{aligned}$$

Hence $|k - \alpha_1| > 1/(2k)^{d-1}$. It follows that if we take $\beta = k - 1/(2k)^{d-1}$ then all eigenvalues of B are strictly less than β in modulus and so

$$\pi_S(k^n) = \mathrm{o}(\beta^n).$$

Then using the inequality $\log(1-x) \leq -x + x^2/2$ for $x \in (0, 1/2)$, we see

$$\log_k(\beta) = 1 + \log(1 - 1/(k \cdot (2k)^{d-1}))/\log(k) \leq 1 - 1/(2k)^{d-1} + 1/2(2k)^{2(d-1)}.$$

We see that

$$\pi_S(k^n) = \mathrm{o}(k^{(1-\epsilon)n})$$

with

$$\epsilon = 1 - 1/(2k)^{d-1} + 1/2(2k)^{2(d-1)}.$$

Then for a given $x > 1$, we have $k^n \leq x < k^{n+1}$ for some n and so

$$\pi_S(x) \leq \pi_S(k^{n+1}) = \mathrm{o}((k^{n+1})^{1-\epsilon}).$$

Since $kx \geq k^{n+1}$ we then see

$$\pi_S(x) = \mathrm{o}(x^{1-\epsilon}),$$

and so we obtain the desired result. □

In general, if k and ℓ are multiplicatively independent, then a sparse k-automatic set can have infinite intersection with an ℓ-automatic set (for example, the set of all integers is ℓ-automatic). But in the case when S is a sparse k-automatic set and T is an ℓ-automatic set of zero density, we again expect $S \cap T$ to be finite. Heuristically, one can see this as follows. Since T has zero density, we have shown that there is some $\epsilon > 0$ such that $\pi_T(x) = \mathrm{o}(x^{1-\epsilon})$ and since S is sparse there are positive constants c and d such that $\pi_S(x) \leq c(\log(x))^d$ for x large. Thus if we take a natural number in $[0, x]$, the probability that it lies in T is at most $x^{-\epsilon}$ for x large. In particular, if $i_1 < i_2 < i_3 < \cdots$ is an enumeration of the elements of our sparse k-automatic set S, then since the bases k and ℓ are multiplicatively independent, we expect that the probability that i_j is in T to be at most $Ci_j^{-\epsilon}$ for some fixed constant C and so the expected number of elements in $S \cap T$ should be bounded by the size of the sum

$$\sum_{j \geq 1} \frac{C}{i_j^{\epsilon}}.$$

Notice that the above series converges when S is sparse. To see this, recall that $\pi_S(x) \leq c(\log(x))^d$ for some $c, d > 0$ and for x large. Since $\pi_S(i_N) = N$, we then have $N \leq c(\log(i_N))^d$

for N large, which gives $i_N \geq \exp((N/c)^{1/d})$ for N sufficiently large. In particular, i_N grows faster than any polynomial in N and so for every $\epsilon > 0$ we have that $\sum_{j\geq 1} 1/i_j^{\epsilon}$ converges.

We conjecture that a much more general phenomenon should hold: for k, ℓ multiplicatively independent positive integers, the intersection of a sparse k-automatic set and a zero density ℓ-automatic set should be finite. Although this problem appears to be well beyond what current methods in number theory can handle, this section (Section 4.2) provides evidence for the conjecture to hold true.

Chapter 5

Additive bases

In this short chapter, we prove a special case of a conjecture of Erdős and Turán [19] for automatic sets, which gives further evidence in support of their conjecture. Some of the exposition is guided by the paper of Bell, Hare, and Shallit [11].

5.1 Automatic sets and additive bases

An important problem in additive number theory is to determine if for a given set S of natural numbers whether there is some $d \geq 2$ such that every natural number can be written as a sum of at most d elements of S (see, e.g., [37]). If such a d exists and this property does not hold for positive numbers smaller than d, we say that S is an *additive basis of order* d for $\mathbb{N}$.

This problem has a long and rich history. Diophantus first asked whether every natural number could be written as a sum of four squares, which was ultimately proved by Lagrange many centuries later. More generally, Waring's problem asks whether the set of k-th powers forms an additive basis for the natural numbers, which was eventually shown to be the case by Hilbert [37, Chapter 3]. Waring's problem is still an active area of research today [32, 45, 47, 46].

Another instance of problems with additive bases is Goldbach's conjecture, which asks whether every even positive integer can be expressed as the sum of at most two prime numbers. If true, this would then imply that every sufficiently large natural number is the sum of at most three prime numbers. Vinogradov [37, Chapter 8] proved that every sufficiently large natural number can be expressed as the sum of at most four prime numbers, and so the set of prime numbers is an additive basis for the natural numbers up to a finite set of exceptions.

Given an additive basis S of order d, we let $r_{S,d}(n)$ denote the number of solutions to $n = s_1 + s_2 + \cdots + s_d$ with $s_1, \ldots, s_d \in S$. Then saying that S is an additive basis of order d gives that $r_{S,d}(n) \geq 1$ for all n. A fundamental problem in the theory of additive bases is the conjecture of Erdős and Turán [19], which asks the following: *Suppose that $S \subseteq \mathbb{N}$ is an additive basis of order $d \geq 2$. Is it true that $\limsup_n r_{S,d}(n) = \infty$?*

This problem is currently open. If one looks at subsets of natural numbers from the point of view of computation then it is natural to ask when an automatic set of natural numbers is an additive basis for $\mathbb{N}$.

Automatic sets that form additive bases were completely characterized by Bell, Hare, and Shallit [11] in the theorem below.

Theorem 73. *Let $k \geq 2$ be a natural number and let S be a k-automatic subset of $\mathbb{N}$. Then S forms an additive basis for $\mathbb{N}$ if and only if the following conditions both hold:*

1. *S is not sparse;*
2. *$1 \in S$.*

Moreover, if S is a non-sparse set and $1 \in S$, then there exists an effectively computable constant N such that every natural number can be expressed as the sum of at most N elements of S.

Using this result, we are able to prove that the Erdős-Turán conjecture holds for automatic sets.

Theorem 74. *Let $k \geq 2$ be a positive integer and let S be a k-automatic subset of $\mathbb{N}$. If S is an additive basis of order d for some $d \geq 2$ then there is a positive constant κ such that $r_{S,2}(N) \geq N^\kappa$ for infinitely many integers N. In particular,*

$$\limsup_n r_{S,d}(n) \to \infty.$$

Proof. By Theorem 73, S cannot be sparse if it is an additive basis. Thus by Proposition 22, we have that S contains a set of the form

$$\{[a\{u_0, u_1\}^* b]_k\},$$

where $a, b, u_0, u_1 \in \Sigma_k^*$ and $t := |u_0| = |u_1| \geq 1$, $u_0 \neq u_1$. Now fix a positive integer n. For each binary word $x := \epsilon_n \cdots \epsilon_1 \in \{0,1\}^*$ of length n, we let $w_x = u_{\epsilon_n} \cdots u_{\epsilon_1}$ and we let $w'_x := u_{1-\epsilon_n} \cdots u_{1-\epsilon_1}$. Then w_x and w'_x are words over Σ_k of length tn and we have 2^{n-1} distinct pairs of such words $\{w_x, w'_x\}$. Now let $[u_0]_k = \gamma_0$, $[u_1]_k = \gamma_1$, and let $[a]_k = \alpha$, $[b]_k = \beta$ and let $|a| = s$, $|b| = r$. Then, by construction, $[aw_xb]_k$ and $[aw'_xb]_k$ are in S for all binary words x of length n and we get 2^{n-1} distinct pairs of natural numbers $\{[aw_xb]_k, [aw'_xb]_k\} \subseteq S$ from this construction. We let $c = \gamma_0 + \gamma_1$. Notice that

$$\begin{aligned}
[aw_xb]_k + [aw'_xb]_k &= [au_{\epsilon_n} \cdots u_{\epsilon_1} b]_k + [au_{1-\epsilon_n} \cdots u_{1-\epsilon_1} b]_k \\
&= \beta + k^b \left(\gamma_{\epsilon_1} + k^t \gamma_{\epsilon_2} + \cdots + k^{t(n-1)} \gamma_{\epsilon_n}\right) + k^{b+tn}\alpha \\
&+ \beta + k^b \left(\gamma_{1-\epsilon_1} + k^t \gamma_{1-\epsilon_2} + \cdots + k^{t(n-1)} \gamma_{1-\epsilon_n}\right) + k^{b+tn}\alpha \\
&= 2\beta + k^b(c + k^t c + \cdots + k^{t(n-1)} c) + 2k^{b+tn}\alpha.
\end{aligned}$$

Thus if we let $N = 2\beta + k^b(c + k^t c + \cdots + k^{t(n-1)} c) + 2k^{b+tn}\alpha$, we see that

$$r_{S,2}(N) \geq 2^{n-1},$$

since we have constructed 2^{n-1} distinct pairs $(s, s') \in S^2$ such that $s + s' = N$. Finally, observe that $N \leq k^{b+tn}(2\beta + 2\alpha + c)$, and so there are positive constants $A, B > 0$ such that $N \leq Ak^{Bn}$. In particular, $\log(N) \leq \log(A) + Bn \log(k)$ and so if C is a constant with $C > B \log(k)$ then for n sufficiently large, we have $\log(N) \leq Cn$. Then, for n large, we have

$$r_{S,2}(N) \geq 2^{n-1} \geq 2^{n/2} \geq 2^{\frac{2}{C} \cdot \log(N)} = N^{\frac{2\log(2)}{C}}.$$

The result now follows by taking $\kappa = \frac{2\log(2)}{C}$. □

Chapter 6

Generalized series with sparse support

6.1 Generalized sparseness

Recall that we introduced generalized series in Section §2.3 and the notion of sparseness in §2.2.

In this chapter, we will extend the notion of sparseness to subsets of $S_k \subseteq \mathbb{Q}$ with $k \geq 2$ a natural number and give a characterization of sparse algebraic generalized series. Following Kedlaya [28], we work with the alphabet $\{0, 1, \ldots, k-1, \bullet\}$, where $\bullet$ represents the radix point in the base-k expansion of a k-adic rational. The set of valid base-k expansions is a regular language [28, Lemma 2.3.2], where such expansions are given by the language

$$\begin{aligned} \mathcal{E}_k := \{&u = u_1u_2\ldots u_n \in \Sigma^* \colon n \geq 1, u_1 \neq 0, u_n \neq 0, \\ &\text{exactly one of } u_1, \ldots, u_n \text{ is equal to } \bullet\}. \end{aligned} \tag{6.1}$$

By definition of sparseness for languages, a sublanguage $\mathcal{L}$ of $\mathcal{E}_k$ is sparse if $f_{\mathcal{L}}(n) = \mathrm{O}(n^d)$ for some $d \geq 1$. If $\mathcal{L}$ is sparse then by Proposition 22, it is a finite union of languages of the form $u_1w_1^*u_2w_2^* \ldots w_s^*u_{s+1}$, where the u_i are possibly trivial and the w_i are non-trivial words. Furthermore by the definition of the language $\mathcal{E}_k$, exactly one of $\{u_1, \ldots, u_{s+1}\}$ contains the radix point and none of the $\{w_1, w_2, \ldots, w_s\}$ can contain the radix point. Hence for a language $u_1w_1^*u_2w_2^* \ldots w_s^*u_{s+1}$, there is a unique index j, $1 \leq j \leq s+1$, such that u_j contains the radix point and so we can write this u_j as $u_j' \bullet u_j''$, and a sparse sublanguage $\mathcal{L}$

of $\mathcal{E}_k$ can be expressed as a finite disjoint union of languages of the form

$$u_1 w_1^* u_2 w_2^* \dots w_{j-1}^* u_j' \bullet u_j'' w_j^* u_{j+1} \dots w_s^* u_{s+1}.$$

For our applications, we will be interested in the case where $k = p$ is prime and we are viewing elements of $\mathcal{E}_p$ as base-p expansions of elements of S_p via the map $[\,\cdot\,]_p$ given in Equation (2.10). In analogy with our definition of sparse subsets of the natural numbers, we will say that a subset of S_p of the form

$$\left\{[u_1 w_1^{n_1} u_2 w_2^{n_2} \dots w_{j-1}^{n_{j-1}} u_j' \bullet u_j'' w_j^{n_j} u_{j+1} \dots w_s^{n_s} u_{s+1}]_p \colon n_1, n_2, \dots, n_s \geq 0\right\}$$

is a *simple sparse* subset of S_p, and we will say that a subset $S \subseteq S_p$ is a *sparse* subset of S_p if S is a finite union of simple sparse subsets of S_p. If $S \subseteq \mathbb{N}$ then it is immediate that being sparse as a subset of S_p exactly coincides with the notion of sparseness introduced for p-automatic subsets of the natural numbers given in Definition 24.

We now shift our focus back to generalized Laurent series. Given a p-quasi-automatic generalized Laurent series $F(t) = \sum_{\alpha \in \mathbb{Q}} f(\alpha) t^\alpha \in \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ with support $S \subseteq \mathbb{Q}$, there is a power q of p such that $f(\alpha) \in \mathbb{F}_q$ by Theorem 48 and there are integers $a > 0$ and b such that $aS + b \subseteq S_p$ and $f_{a,b} : S_p \to \mathbb{F}_q$ given by $f_{a,b}(x) = f((x-b)/a)$ is p-automatic in the sense of Definition 47. We will say that $F(t)$ is a *sparse generalized Laurent series* if $aS + b \subseteq S_p$ is a sparse subset of S_p, where a and b are as above.

Lemma 75. *Let $S \subseteq S_p$ be p-automatic. Then S is sparse if and only if*

$$\#\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} = \mathrm{O}(n^d)$$

for some positive integer d.

Proof. Let $\mathcal{L} \subseteq \mathcal{E}_k$ be the regular language $\{(x)_p \colon x \in S\}$. Then S is sparse if and only if $\mathcal{L}$ is sparse. Notice that

$$\#\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} = \#\{u \bullet v \in \mathcal{L} \colon \mathrm{length}(u), \mathrm{length}(v) \leq n\}.$$

The set $\{u \bullet v \in \mathcal{L} \colon \mathrm{length}(u), \mathrm{length}(v) \leq n\}$ is a subset of the set of words in $\mathcal{L}$ of length at most $2n+1$ and so if $\mathcal{L}$ is sparse, $\#\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} = \mathrm{O}(n^d)$ for some $d \geq 0$. Conversely, if $\mathcal{L}$ is not sparse, then it contains a sublanguage of the form $u\{y,z\}^* v$, where exactly one of u and v contains the radix point. Let κ denote the maximum of the lengths of y and z. Then in either case, every element of the form $[uwv]_p$, with w a word in $\{y,z\}^*$ of length at most $(2\kappa)^{-1} n$, is in $\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\}$ for n sufficiently large. Since the number of words of length at most $(2\kappa)^{-1} n$ in $\{y,z\}^*$ grows exponentially in n, $\#\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} \neq \mathrm{O}(n^d)$ when $\mathcal{L}$ is not sparse. □

Definition 76. Let S be a (not necessarily p-automatic) subset of S_p. We say that S is *weakly sparse* if

$$\#\{a \in S \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} = \mathrm{O}(n^d)$$

for some positive integer d. In particular, a subset of S_p is sparse if and only if it is p-automatic and weakly sparse, and an automatic subset of a weakly sparse set is sparse.

The following remark follows immediately from Lemma 75.

Lemma 77. *If a, a' and b, b' are rational numbers with $a, a' > 0$ then if $S \subset \mathbb{Q}$ has the property that both $aS + b$ and $a'S + b'$ lie in S_p then $aS + b$ is sparse if and only if $a'S + b'$ is sparse, and so this definition of sparseness does not depend upon the choice of affine transformation that we use to push S into the p-adic rationals.*

Before the next remark, we recall that $\mathbb{Z}_{(p)}$ is the subring of rational numbers of the form a/b with a, b integers and $p \nmid b$.

Remark 78. *Let p be a prime number and let S be a non-empty well-ordered simple sparse subset of S_p. Then there exist $s \geq 0$, $c_0, \ldots, c_{j-1} \in \mathbb{Z}_{(p)}$, $d_{j-1}, \ldots, d_s \in \mathbb{Q}$, and positive integers $\delta_1, \ldots, \delta_s$ such that*

$$\begin{aligned} S = \{ & c_0 + c_1 p^{\delta_{j-1} n_{j-1}} + c_2 p^{\delta_{j-1} n_{j-1} + \delta_{j-2} n_{j-2}} \cdots + c_{j-1} p^{\delta_{j-1} n_{j-1} + \cdots + \delta_1 n_1} \\ & + d_{j-1} + d_j p^{-\delta_j n_j} + d_{j+1} p^{-(\delta_j n_j + \delta_{j+1} n_{j+1})} + \cdots + d_s p^{-(\delta_j n_j + \cdots + \delta_s n_s)} \colon n_1, \ldots, n_s \geq 0\}. \end{aligned} \tag{6.2}$$

Furthermore, we have

$$c_1 p^{\delta_{j-1} n_{j-1}} + c_2 p^{\delta_{j-1} n_{j-1} + \delta_{j-2} n_{j-2}} \cdots + c_{j-1} p^{\delta_{j-1} n_{j-1} + \cdots + \delta_1 n_1} \geq 0$$

for all $n_1, \ldots, n_{j-1} \geq 0$ and

$$d_j p^{-\delta_j n_j} + d_{j+1} p^{-(\delta_j n_j + \delta_{j+1} n_{j+1})} + \cdots + d_s p^{-(\delta_j n_j + \cdots + \delta_s n_s)} \leq 0$$

for all $n_j, \ldots, n_s \geq 0$.

Proof. Let $[u_i]_p = a_i$ and $\mu_i = \text{length}(u_i)$ for $i \in \{1, \ldots, s\} \setminus \{j\}$, $[u'_j]_p = a'_j$, $[u''_j]_p = a''_j$, $\mu'_j = \text{length}(u'_j)$, $\mu''_j = \text{length}(u''_j)$, and $[w_i]_p = b_i$ and $\delta_i = \text{length}(w_i)$ for $i = 1, \ldots, s$. The pre-radix part can be handled as in Lemma 33 and the post-radix part is handled similarly as follows. Putting $d_{j-1} = a''_j - \frac{b_j p^{-\mu''_j}}{p^{-\delta_j} - 1}$, $d_j = \frac{p^{-\mu''_j} b_j}{p^{-\delta_j} - 1} + p^{-\mu''_j} a_{j+1} - \frac{b_{j+1} p^{-\mu''_j - \mu_{j+1}}}{p^{-\delta_{j+1}} - 1}$,

$\ldots$, $d_s = p^{-\mu_j''-\mu_{j+1}-\cdots-\mu_s}a_{s+1} + \frac{b_s p^{-\mu_j''-\mu_{j+1}-\cdots-\mu_s}}{p^{-\delta_s}-1}$, we get the desired description of S. The inequalities

$$c_1 p^{\delta_{j-1}n_{j-1}} + c_2 p^{\delta_{j-1}n_{j-1}+\delta_{j-2}n_{j-2}} \cdots + c_{j-1} p^{\delta_{j-1}n_{j-1}+\cdots+\delta_1 n_1} \geq 0$$

for all $n_1, \ldots, n_{j-1} \geq 0$ and

$$d_j p^{-\delta_j n_j} + d_{j+1} p^{-(\delta_j n_j + \delta_{j+1} n_{j+1})} + \cdots + d_s p^{-(\delta_j n_j + \cdots + \delta_s n_s)} \leq 0$$

for all $n_j, \ldots, n_s \geq 0$ follow from the fact that S is well-ordered. To obtain the first inequality, suppose that

$$\Psi(n_1, \ldots, n_{j-1}) := c_1 p^{\delta_{j-1}n_{j-1}} + c_2 p^{\delta_{j-1}n_{j-1}+\delta_{j-2}n_{j-2}} \cdots + c_{j-1} p^{\delta_{j-1}n_{j-1}+\cdots+\delta_1 n_1} < 0$$

for some $n_1, \ldots, n_{j-1} \geq 0$. Then since

$$\Psi(n_1, \ldots, n_{j-1} + a) = p^{\delta_{j-1}a}\Psi(n_1, \ldots, n_{j-1})$$

for $a \geq 0$ and $\delta_{j-1} > 0$, we obtain an infinite descending subsequence in S, contradicting the fact that it is well-ordered. The second inequality follows in a similar manner. □

The collection of sparse series forms a subalgebra of the ring of algebraic power series with coefficients in $\bar{\mathbb{F}}_p$. This is in fact rather straightforward, but for the sake of completeness, we include a proof (see Proposition 82); in addition, we show that sparse series possess natural closure properties, which we detail below.

Definition 79. Let $B \subseteq C$ be subalgebras of the ring of generalized Laurent series $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$. We say that B is *Artin-Schreier closed in C* if the following hold:

(P1) if $F(t) \in B$ and if $G(t) \in C$ is a solution to the equation $X^p - X + F(t) = 0$, then $G(t) \in B$;

(P2) If $F(t) \in B$ and $\alpha \in \bar{\mathbb{F}}_p$ then $F(\alpha t) \in B$;

(P3) if $F(t) \in B$, $c \in \mathbb{Q}_{>0}$ and $d \in \mathbb{Q}$, and $t^d F(t^c) \in C$, then $t^d F(t^c) \in B$.

We make a remark concerning property (P1). In general, a generalized Laurent series $F(t)$ can be written as $F_+(t) + c + F_-(t)$, where c is constant, $F_+ \in \bar{\mathbb{F}}_p[[t^{\mathbb{Q}}]]_{>0}$ and $F_-(t) \in \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))_{<0}$. Then there is some $a \in \bar{\mathbb{F}}_p$ such that $a^p - a = c$ and all solutions to $X^p - X = -F(t)$ are of the form $G_+(t) + G_-(t) + a + i$, where $i \in \mathbb{F}_p$, $G_+(t) =$

$F_+(t) + F_+(t^p) + F_+(t^{p^2}) + \cdots$ and $G_-(t) = -F_-(t^{1/p}) - F_-(t^{1/p^2}) - \cdots$. In the case when C is the ring of formal power series and B is a subalgebra of C, condition (P1) simply says that if $F(t) \in B$ and $F(0) = 0$ then $F(t) + F(t^p) + F(t^{p^2}) + \cdots$ is also in B. Our goal is to show that various rings of sparse algebraic series are Artin-Schreier closed in natural overrings. To do this, we need a quick lemma about sparse subsets of S_p.

Lemma 80. *Let p be prime, let b be a positive integer and let $S \subseteq S_p$ be a well-ordered sparse set. Then we have the following:*

(a) $S \cap [0, b)$ and $S \cap (b, \infty)$ are both sparse;

(b) if $T := S \cap (b, \infty)$ then $\bigcup_{n \geq 0} ((T - b)p^n + b)$ is a well-ordered sparse set;

(c) if $U := S \cap [0, b)$ then $\bigcup_{n \geq 1} ((U - b)p^{-n} + b)$ is a well-ordered sparse set.

Proof. To prove (a), let $S \subseteq S_p$ be a sparse set. Applying the map $(\,\cdot\,)_p$ to S we obtain a sparse regular language $\mathcal{L} \subseteq \mathcal{E}_p$. Both $S_p \cap [0, b)$ and $S_p \cap (b, \infty)$ correspond to regular languages and hence $S \cap [0, b)$ and $S \cap (b, \infty)$ correspond to regular languages as well. Moreover, since they are sublanguages of the sparse language $\mathcal{L}$, both $S \cap [0, b)$ and $S \cap (b, \infty)$ are sparse.

We now prove part (b). By part (a), we know that T is sparse. By Lemma 77, affine transformations preserve sparseness, so $T' := T - b$ is a well-ordered sparse set. Since T' is a finite disjoint union of simple sparse sets, it is no loss of generality to assume that T' is a simple sparse set in what follows. We let $\mathcal{L}_{T'}$ denote the sublanguage of $\mathcal{E}_p$ obtained by applying $(\,\cdot\,)_p$ to T'. Then since we are assuming that T' is simple sparse, $\mathcal{L}_{T'}$ is a language of the form

$$u_1 w_1^* u_2 w_2^* \ldots w_{j-1}^* u'_j \bullet u''_j w_j^* u_{j+1} \ldots w_s^* u_{s+1}.$$

Consequently, the sublanguage of $\mathcal{E}_p$ obtained by applying $(\,\cdot\,)_p$ to $\bigcup p^n T'$ is a finite union of languages of the form

(i) $u_1 w_1^* u_2 w_2^* \cdots u_s w_s^* u_{s+1} 0^* \bullet$;

(ii) $u_1 w_1^* u_2 w_2^* \ldots w_{j_0-1}^* u'_{j_0} \bullet u''_{j_0} w_{j_0}^* u_{j_0+1} \ldots w_s^* u_{s+1}$; and

(iii) $u_1 w_1^* u_2 w_2^* \ldots w_{i_0-1}^* u_{i_0} w_{i_0}^* w'_{i_0} \bullet w''_{i_0} w_{i_0}^* u_{i_0+1} \ldots w_s^* u_{s+1}$, where $i_0 \in \{j, \ldots, s\}$ and $w'_{i_0} w''_{i_0} = w_{i_0}$, and $j_0 \in \{j, \ldots, s+1\}$, $u'_{j_0} u''_{j_0} = u_{j_0}$, and if $j_0 = j$ then u'_{j_0} has u'_j as a prefix. Hence $\bigcup p^n T'$ is a sparse set and since affine transformations preserve sparseness, we have

$$b + \bigcup p^n T' = \bigcup_{n \geq 0} \left((T-b)p^n + b\right)$$

is sparse. To see that $\bigcup_{n \geq 0} \left((T-b)p^n + b\right)$ is well-ordered, it suffices to show that the union of $p^n T'$ is well-ordered. Let $t_0 > 0$ denote the smallest element of T' and suppose that $x_1 \geq x_2 \geq \cdots$ is a weakly decreasing chain in the union of the sets $p^n T'$. Then there is some $N > 0$ such that $x_1 < p^N t_0$ and hence $x_1, x_2, x_3, \ldots$ must be contained in the finite union $\bigcup_{i<N} p^i T'$, which is well-ordered, as it is a finite union of well-ordered subsets of $\mathbb{Q}$, and so the chain $x_1 \geq x_2 \geq \cdots$ necessarily terminates. Thus we have established part (b).

Finally, we prove part (c). The proof that $U' := \bigcup_{n \geq 1} \left((U-b)p^{-n} + b\right)$ is well-ordered is done exactly as in the proof of part (b). Thus it only remains to show that this set is sparse. We write $U = \bigcup_{a=0}^{b-1} U_a$, where $U_a = \{x \in U \colon a \leq x < a+1\}$. Then every element in U_a has a base-p expansion of the form $(a)_p \bullet w$, where w lies in a sparse sublanguage $\mathcal{C}_a$ of $\{0, 1, \ldots, p-1\}^*$. Then $b - U_a = (b - (a+1)) + \{1 - [{\bullet} w]_p \colon w \in \mathcal{C}_a\}$. Since $\mathcal{C}_a$ is sparse, it is a finite union of simple sparse languages. Observe, moreover, that if $x \in [0,1) \cap S_p$ is a number having base-p expansion ${\bullet}\, v_1 w_1^* v_2 w_2^* \cdots v_s w_s^* v_{s+1}$, with v_{s+1} non-empty, then $1 - x$ has base-p expansion

$${\bullet} \bar{v}_2 \bar{w}_1^* \bar{v}_2 \bar{w}_2^* \cdots \bar{v}_s \bar{w}_s^* \tilde{v}_{s+1},$$

where if $u = a_1 a_2 \ldots a_d$, $d \geq 1$, we define $\bar{u} := (p-1-a_1)(p-1-a_2)\ldots(p-1-a_d)$ and $\tilde{u} := (p-1-a_1)(p-1-a_2)\ldots(p-1-a_{d-1})(p-a_d)$. In general, if v_{s+1} is empty, one can get a similar description of the set of $1-x$ and, in this way, one can show that $\{1 - [{\bullet} w]_p \colon w \in \mathcal{C}_a\}$ is sparse (although it need not be well-ordered). Thus $b - U = \bigcup_{a=0}^{b-1} (b - U_a)$ is sparse. Now we write

$$b - U = \bigcup_{0 \leq a < b} \left(a + [\,{\bullet}\, \mathcal{D}_a]_p\right),$$

where each $\mathcal{D}_a$ is a sparse sublanguage of $\{0, 1, \ldots, p-1\}^*$. If the base p-expansion of a is equal to $a_1 \cdots a_r$, then

$$\bigcup_{n \geq 1} p^{-n} \left(a + [\,{\bullet}\, \mathcal{D}_a]_p\right) = \bigcup_{i=0}^{\infty} [\,{\bullet} 0^i a_1 \cdots a_r \,{\bullet}\, \mathcal{D}_a]_p \cup \bigcup_{i=1}^{r} [a_1 a_2 \ldots a_i \,{\bullet}\, a_{i+1} \ldots a_r \mathcal{D}_a]_p,$$

which is a finite union of simple sparse sets, because $\mathcal{D}_a$ is a finite union of simple sparse languages. Hence $\bigcup_{n \geq 0} (b - U) p^{-n}$ is a finite union of sparse sets and thus is itself sparse.

Now

$$U' = \bigcup_{n\geq 1} \big((U-b)p^{-n}+b\big) = b - \bigcup_{n\geq 1}(b-U)p^{-n} \subseteq [0,b),$$

which is sparse by the same argument as above. The result follows. □

We need one more basic fact.

Lemma 81. *Let $S, T \subseteq S_p$ be well-ordered sparse sets. Then $S \cup T$ and $S+T$ are well-ordered sparse.*

Proof. First we show that $S \cup T$ and $S+T$ are well-ordered. By assumption, both S and T are well-ordered subsets of $\mathbb{Q}$. If $S+T$ is not well-ordered, then by Remark 46 there exists an infinite decreasing sequence $x_1 > x_2 > \cdots$ within $S+T$ where $x_n = s_n + t_n$ for all $n \geq 1$. We can construct a subsequence s_{n_k} of s_n as follows: define $s_{n_1} = \min\{s_n\}$ and $s_{n_{j+1}} = \min\{s_n : n > n_j\}$. Then we have $n_1 < n_2 < \cdots$ and $s_{n_1} \leq s_{n_2} \leq \cdots$. Since $\{x_n\}_{n=1}^{\infty}$ is a decreasing sequence, we have $t_{n_1} > t_{n_2} > \cdots$, an infinite decreasing sequence within T, which is a contradiction since T is well-ordered. To show that $S \cup T$ is well-ordered, let X be a nonempty subset of $S \cup T$. We can write $X = (X \cap S) \cup (X \cap T)$. Denote by x_s a minimal element of $X \cap S$ and by x_t a minimal element of $X \cap T$. Then $\min\{x_s, x_t\}$ is a minimal element of X, and so $S \cup T$ is well-ordered.

By Proposition 49, both $S \cup T$ and $S+T$ are p-automatic. So there only remains to show sparseness. Since sparse sets can be decomposed as a finite union of simple sparse sets, and since a finite union of simple sparse sets is sparse, we see $S \cup T$ is sparse. We now show that $S+T$ is weakly sparse, from which it will immediately follow that $S+T$ is sparse. Since a finite union of weakly sparse sets is weakly sparse and since S and T are finite unions of simple sparse sets, we may assume without loss of generality that S and T are simple sparse.

A simple sparse subset of S_p is of the form $\{[u_{\bullet}v]_p \colon u \in \mathcal{L}, v \in \mathcal{L}'\}$ where $\mathcal{L}, \mathcal{L}'$ are simple sparse sublanguages of $\{0,1,\ldots,p-1\}^*$. In particular, $S = A + X$, where A is a sparse subset of $\mathbb{N}$ and X is a well-ordered sparse subset of $S_p \cap [0,1)$. Similarly, $T = B + Y$, where B is a sparse subset of $\mathbb{N}$ and Y is a sparse well-ordered subset of $S_p \cap [0,1)$. Hence $S+T = (A+B)+(X+Y)$. Since A and B are sparse sets of natural numbers, and since $\pi_{A+B}(x) \leq \pi_A(x)\pi_B(x)$, we see that $\pi_{A+B}(x) = \mathrm{O}((\log x)^d)$ for some $d \geq 0$. In particular, since a sum of two p-automatic subsets of natural numbers is again a p-automatic set of natural numbers [2, Theorem 5.6.3], $A+B$ is a sparse p-automatic subset of $\mathbb{N}$. Now let $\mathcal{L} \subseteq \mathcal{E}_p$ be the regular language $\{(x)_p \colon x \in S+T\}$. Since $X+Y \subseteq [0,2)$ and is well-ordered, if $u_{\bullet}v \in \mathcal{L}$ then $[u]_p \in (A+B) \cup (A+B+1)$ for $u_{\bullet}v \in \mathcal{L}$; moreover, by Kedlaya's description of post-radix behaviour always being sparse [28, Theorem 7.1.6], there is a sparse p-automatic subset Z of $S_p \cap [0,1)$ such that $\{[v]_p \colon u\,\bullet\, v \in \mathcal{L}\} = Z$. Thus

$$\#\{a \in S+T \colon a < p^n \text{ and } p^n a \in \mathbb{N}\} \leq \pi_{(A+B)\cup(A+B+1)}(p^n) \cdot \#\{a \in Z \colon p^n a \in \mathbb{N}\}.$$

Then by the above remarks and Lemma 75, both $\pi_{(A+B)\cup(A+B+1)}(p^n)$ and $\#\{a \in Z \colon p^n a \in \mathbb{N}\}$ are bounded by polynomials in n and thus we obtain the result by Lemma 75. □

Proposition 82. *Let p be prime. Then we have the following:*

(a) the collection of sparse algebraic power series in $\bar{\mathbb{F}}_p[[t]]$ forms a subalgebra of the ring of algebraic power series; moreover this subalgebra is Artin-Schreier closed in $\bar{\mathbb{F}}_p[[t]]$;

(b) the collection of sparse algebraic generalized series in $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ forms a subalgebra of the ring of generalized Laurent series; moreover this subalgebra is Artin-Schreier closed inside $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$.

Proof. We let A denote the collection of sparse algebraic power series in $\bar{\mathbb{F}}_p[[t]]$. Then to show that A is a subalgebra, it is sufficient to show that it is closed under summation and multiplication. Let $F(t), G(t) \in A$ and let S_F and S_G denote the supports of F and G respectively. Then the support of $(F+G)(t)$ is contained in $S_F \cup S_G$ and since S_F and S_G are sparse then we see from the characterization of sparseness given in Theorem 23 that $S_F \cup S_G$ is sparse and so $F+G$ is a sparse algebraic power series. The support of $F(t)G(t)$ is contained in $S_F + S_G$, where $S_F + S_G$ is the collection of natural numbers that can be expressed in the form $a+b$ with $a \in S_F$ and $b \in S_G$. If we define $\pi_S(x) = \#\{n \leq x \colon n \in S\}$ for $x \geq 0$ for a subset S of the natural numbers, then $\pi_{S_F+S_G}(x) \leq \pi_{S_F}(x)\pi_{S_G}(x)$ and so again from the characterization of sparseness given in Theorem 23, $F(t)G(t)$ is a sparse algebraic power series. The only property from $(P1)$–$(P3)$ in Definition 79 that does not obviously hold for sparse series is property (P1). Suppose that $F(t)$ is a sparse series with $F(0) = 0$ and let S be the support of F. Then if we let S' denote the support of $G(t) := F(t) + F(t^p) + \cdots$, then we see that S' is contained in $T := \cup_{n\geq 0}(p^n \cdot S)$. Then if we look at the language $\mathcal{L} := \{(n)_k \colon n \in S\}$ then $\{(n)_k \colon n \in S'\} \subseteq \mathcal{L} \cdot \{0\}^*$, which is sparse by Equations (2.5) and (2.6). Since sparse languages are closed under the process of taking regular sublanguages, the support of $G(t)$ is sparse.

For part (b), we must show that if $F(t), G(t) \in \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ are sparse then so are $F(t)+G(t)$ and $F(t)G(t)$. Let S_F and S_G denote the supports of F and G respectively. After replacing F and G by $t^b F(t^a)$ and $t^b G(t^a)$ for some positive rational numbers a and b, we may assume that $S_F, S_G \subseteq S_p$. Then the supports of $F(t)+G(t)$ and $F(t)G(t)$ are contained in

$S_F \cup S_G$ and $S_F + S_G$ respectively, and since the supports of $F(t) + G(t)$ and $F(t)G(t)$ are p-automatic and well-ordered, we then see they are sparse by Lemma 81.

To show the property of being Artin-Schreier closed holds, it is again enough to prove that (P1) holds. Let $F(t)$ be a sparse generalized power series and again let S denote its support. By assumption there are integers a and b with $a, b > 0$ such that $T := Sa + b \subseteq S_p$ is automatic, sparse, and well-ordered. By Lemma 80, $T_+ := T \cap (b, \infty)$ and $T_- := T \cap [0, b)$ are both sparse automatic subsets of S_p. Let $S_+ = (T_+ - b)/a$ and $S_- = (T_- - b)/a$. By the remarks following Definition 79, if $G(t)$ is a solution to the equation $X^p - X + F(t) = 0$ and if U denotes the support of G, then U is contained in the union of $S_1 := \bigcup_{n\geq 0} p^n S_+$, $S_2 := \bigcup_{n\geq 1} p^{-n} S_-$, and $\{0\}$. Now, let $T_1 = S_1 a + b \subseteq S_p$ and let $T_2 = S_2 a + b$. Then since automatic subsets of sparse sets are sparse, it suffices to show that T_1 and T_2 are sparse. But $T_1 = \bigcup_{n\geq 0}((T_+ - b)p^n + b)$ and $T_2 = \bigcup_{n\geq 1}((T_- - b)p^{-n} + b)$, so T_1 and T_2 are sparse by Lemma 80, and so the result follows. □

We make the following remark. We recall that given a field K and $F(t) = \sum f(n)t^n$, $G(t) = \sum g(n)t^n \in K[[t]]$, the Hadamard product of F and G is the series $\sum_{n\geq 0} f(n)g(n)t^n$. Then it is well-known that algebraic power series are closed under Hadamard product (see [2, Theorem 12.2.6]) and since the support of the Hadamard product of two series is the intersection of the supports of the series, the following remark is immediate.

Remark 83. *Let p be a prime and let q be a power of p. The ring of sparse algebraic power series in $\bar{\mathbb{F}}_p[[t]]$ is closed under Hadamard product.*

6.2 Proof of the main theorem for sparse Kedlaya

In this section, we give the proof of Theorem 3. In fact, we will prove a somewhat more general version of Theorem 3 that deals with Kedlaya's extension of Christol's theorem. Before giving this more general statement, we find it convenient to fix the following notation.

Notation 84. *We adopt the following notation:*

(1) we let p be prime and we let q be a power of p;

(2) we let $K = \bar{\mathbb{F}}_p(t^{1/n} : n \geq 1, p \nmid n)$;

(3) we let R denote $\mathbb{F}_p[t^{\pm 1/n} : n \geq 1, p \nmid n]$;

(4) we let L denote the compositum of all Galois extensions of K of order a power of p;

(5) we let L_0 denote the elements $G \in L$ such that $K[G(t)]/K$ is unramified outside 0 and ∞;

(6) for each $\lambda \in \mathbb{P}^1_{\bar{\mathbb{F}}_p}$, we let ν_λ be the valuation of K induced by taking the order of vanishing at $t = \lambda$ (this valuation is discrete when $\lambda \in \bar{\mathbb{F}}_p^* = \mathbb{P}^1 \setminus \{0, \infty\}$);

(7) given a finite Galois extension E of K, we let $\mathcal{V}_E \subseteq E$ be the set of elements $a \in E$ such that $\nu(a) \notin \{-p, -2p, -3p, \ldots\}$ for all rank-one discrete valuations ν of E with $\nu|_K = \nu_\lambda$ for some $\lambda \in \bar{\mathbb{F}}_p^*$;

(8) given a finite Galois extension E of K, we let $\mathcal{V}_{E,+} \subseteq E$ denote the set of elements $a \in E$ such that $\nu(a) \geq 0$ for all discrete valuations ν of E with $\nu|_K = \nu_\lambda$ for some $\lambda \in \bar{\mathbb{F}}_p^*$;

(9) we let C denote the smallest non-trivial $\bar{\mathbb{F}}_p$-subalgebra of $\bar{\mathbb{F}}_p[[t]]$ that is Artin-Schreier closed in the power series ring $\bar{\mathbb{F}}_p[[t]]$;

(10) we let $\widetilde{C}$ denote the smallest non-trivial $\bar{\mathbb{F}}_p$-subalgebra of $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ that is Artin-Schreier closed in the generalized Laurent series ring $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$;

(11) we let B denote the collection of generalized power series $G(t)$ such that for some $j \geq 0$, $G(t^{p^j}) \in L_0$ and is integral over R;

(12) we let A denote the ring of sparse algebraic power series and we let $\widetilde{A}$ denote the ring of sparse algebraic generalized Laurent series.

In terms of generalized series, we have the following more general version of Theorem 3.

Theorem 85. *Let p be prime and adopt the notation of Notation 84. Then*

$$\widetilde{A} = B = \widetilde{C}.$$

In terms of the above notation, Theorem 3 can be stated as $A = B \cap \bar{\mathbb{F}}_p[[t]] = C$, and so Theorem 85 is an extension of Theorem 3 in the setting of generalized Laurent series.

First, we prove the equalities $A = C$ and $\widetilde{A} = \widetilde{C}$. Proposition 82 shows that A is Artin-Schreier closed in $\bar{\mathbb{F}}_p[[t]]$ and that $\widetilde{A}$ is Artin-Schreier closed in $\bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$. In particular, we already have shown that we have the containments $C \subseteq A$ and $\widetilde{C} \subseteq \widetilde{A}$. Thus the main content is to prove the reverse inclusion. The key result in this direction is Lemma 87. Before the key lemma, we recall Alon's Combinatorial Nullstellensatz.

Theorem 86. *Let K be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $K[x_1, \ldots, x_n]$. Suppose the degree of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of K with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that*

$$f(s_1, \ldots, s_n) \neq 0.$$

Proof. See [5, Theorem 1.2]. □

Lemma 87. *Adopt the notation of Notation 84 and let $d \geq 1$. Then we have the following:*

(i) if $F(t) \in C$ and $F(0) = 0$ then $F(t) + F(t)^{p^d} + F(t)^{p^{2d}} + \cdots \in C$;

(ii) if $F(t) \in \widetilde{C} \cap \bar{\mathbb{F}}_p[[t^{\mathbb{Q}}]]_{>0}$ then $F(t) + F(t)^{p^d} + F(t)^{p^{2d}} + \cdots \in \widetilde{C}$ and if $F(t) \in \widetilde{C} \cap \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))_{<0}$ then $F(t)^{p^{-d}} + F(t)^{p^{-2d}} + F(t)^{p^{-3d}} + \cdots \in \widetilde{C}$.

Proof. (i) Let $d \geq 1$ and let $x_1, \ldots, x_d$ be commuting indeterminates. We let $A(x_1, \ldots, x_d) \in M_d(\mathbb{F}_p[x_1, \ldots, x_d])$ be the matrix whose (i,j)-entry is $x_i^{p^{j-1}}$. Then $f := \det(A(x_1, \ldots, x_d))$ is a homogeneous polynomial in the variables $x_1, \ldots, x_d$ of total degree $p^{d-1} + \cdots + p + 1$ with the property that the coefficient of

$$\prod_{i=1}^{d} x_i^{p^{i-1}}$$

is nonzero. By Theorem 86, there is some $(a_1, \ldots, a_d) \in \bar{\mathbb{F}}_p^d$ such that $\det(A(a_1, \ldots, a_d)) \neq 0$, since p^d is greater than the degree of f. Now let $B = A(a_1, \ldots, a_d)$. By construction $\det(B)$ is nonzero, and so there is some $(c_1, \ldots, c_d) \in \bar{\mathbb{F}}_p^{1\times d}$ such that $(c_1, \ldots, c_d)B = (1, 0, 0, \ldots, 0)$. In other words, $\sum_{i=1}^{d} c_i a_i^{p^j} = \delta_{j,0}$ for $j = 0, 1, \ldots, d-1$. Moreover, since $a_i^{p^d} = a_i$ for $i = 1, \ldots, d$, we in fact have

$$\sum_{i=1}^{d} c_i a_i^{p^j} = \begin{cases} 1 & \text{if } j \equiv 0 \pmod{d}, \\ 0 & \text{otherwise.} \end{cases}$$

For $i = 1, \ldots, d$, we let $H_i(t) = a_i F(t) + a_i^p F(t)^p + \cdots$. Then since $a_i F(t) \in C$ and C is Artin-Schreier closed, we have $H_i(t) \in C$ for $i = 1, \ldots, d$. Thus

$$\sum_{i=1}^{d} c_i H_i(t) = F(t) + F(t)^{p^d} + F(t)^{p^{2d}} + \cdots \in C.$$

(ii) The first assertion is handled similar to part (i). For the proof of second assertion, we again can find $c_i \in \bar{\mathbb{F}}_p$, $i = 1, \ldots, d$ such that $\sum_{i=1}^{d} c_i a_i^{p^j} = \delta_{j,0}$ for $j = 0, 1, \ldots, d-1$, which can be rewritten as $\sum_{i=1}^{d} c_i a_i^{p^{d-k}} = \delta_{d-k,0}$ for $k = 0, 1, \ldots, d-1$. Then since $a_i^{1/p} = a_i^{p^{d-1}}$ for each i,

$$\sum_{i=1}^{d} c_i a_i^{p^{-k}} = \begin{cases} 1 & \text{if } k \equiv 0 \pmod{d}, \\ 0 & \text{otherwise.} \end{cases}$$

For $i = 1, \ldots, d$, we let $H_i(t) = a_i F(t) + a_i^p F(t)^p + \cdots$. Then since $a_i F(t) \in C$ and C is Artin-Schreier closed, we have $H_i(t) \in C$ for $i = 1, \ldots, d$. Thus

$$\sum_{i=1}^{d} c_i H_i(t) = F(t) + F(t)^{p^d} + F(t)^{p^{2d}} + \cdots \in C.$$

For $i = 1, \ldots, d$, we let $H_i(t) = a_i^{1/p} F(t)^{1/p} + a_i^{1/p^2} F(t)^{1/p^2} + \cdots$. Then since $a_i^{1/p} F(t)^{1/p} \in \tilde{C}$ and $\tilde{C}$ is Artin-Schreier closed, we have $H_i(t) \in \tilde{C}$ for $i = 1, \ldots, d$. Therefore

$$\sum_{i=1}^{d} c_i H_i(t) = F(t)^{-p^d} + F(t)^{-p^{2d}} + \cdots \in \tilde{C}.$$

□

We next require a lemma concerning power series whose support set is a simple sparse set.

Lemma 88. *Let p be prime and adopt the notation of Notation 84. Then the following hold:*

(i) if $S \subseteq \mathbb{N}$ is a non-empty simple sparse subset of $\mathbb{N}$, then

$$G(t) := \sum_{n \in S} t^n \quad \textit{is in } C,$$

(ii) if $S \subseteq S_p$ is a non-empty well-ordered simple sparse subset of S_p, then

$$G(t) := \sum_{\alpha \in S} t^\alpha \quad \textit{is in } \widetilde{C}.$$

Proof. We first give the proof of (i). By Lemma 33, there is some $s \geq 0$ and some $c_0, \ldots, c_s \in \mathbb{Z}_{(p)}$ and positive integers $\delta_1, \ldots, \delta_s$ such that

$$S = \left\{c_0 + c_1 p^{\delta_s n_s} + \cdots + c_s p^{\delta_1 n_1 + \cdots + \delta_s n_s} : n_1, \ldots, n_s \geq 0\right\}.$$

Moreover, we have $n \geq c_0$ for all $n \in S$ and $c_0 \in S$ if and only if $s = 0$. We prove that $G(t) \in C$ by induction on s. When $s = 0$, $G(t)$ is a monomial and the result is clear. Thus we suppose that the result holds whenever $s < m$ with $m \geq 1$ and we consider the case when $s = m$.

Then we may assume that S is a set of natural numbers of the form

$$\left\{c_0 + c_1 p^{\delta_m n_m} + \cdots + c_m p^{\delta_1 n_1 + \cdots + \delta_m n_m} : n_1, \ldots, n_m \geq 0\right\}.$$

We pick a positive integer N that is coprime to p such that $c_i N \in \mathbb{Z}$ for $i = 0, \ldots, m$. We let

$$T = \left\{Nc_1 + Nc_2 p^{\delta_{m-1} n_{m-1}} + \cdots + Nc_m p^{\delta_1 n_1 + \cdots + \delta_{m-1} n_{m-1}} : n_1, \ldots, n_{m-1} \geq 0\right\}.$$

Then T is a subset of the integers and since $m > 1$, every $n \in S$ is strictly greater than c_0 and so T is a sparse subset of the positive integers. We let $H(t) = \sum_{n \in T} t^n$. Then by the induction hypothesis $H(t) \in C$. We have

$$G(t^N) = \sum_{n \in N \cdot S} t^n = t^{Nc_0} \sum_{j \geq 0} \left(\sum_{n \in T} t^n\right)^{p^{j\delta_m}}.$$

That is, $G(t^N) = t^{Nc_0}\left(\sum_{j \geq 0} H(t)^{p^{j\delta_m}}\right)$. By Lemma 87,

$$\sum_{j \geq 0} H(t)^{p^{j\delta_m}} \in C.$$

Since $G(t^N)$ is a power series and C is Artin-Schreier closed in $\bar{\mathbb{F}}_p[[t]]$, it follows that

$$G(t^N) = t^{Nc_0}\left(\sum_{j\geq 0} H(t)^{p^{j\delta_m}}\right) \in C.$$

Since $G(t)$ is also a power series and C is Artin-Schreier closed in $\bar{\mathbb{F}}_p[[t]]$, we have $G(t) \in C$. The result follows.

The proof of (ii) is handled in a similar manner. We use Remark 78 to show that if $S \subseteq S_p$ is a non-empty well-ordered simple sparse set of the form

$$\begin{aligned}\{&c_0 + c_1 p^{\delta_{j-1}n_{j-1}} + c_2 p^{\delta_{j-1}n_{j-1}+\delta_{j-2}n_{j-2}} \cdots + c_{j-1}p^{\delta_{j-1}n_{j-1}+\cdots+\delta_1 n_1} \\ &+ d_{j-1} + d_j p^{-\delta_j n_j} + d_{j+1}p^{-(\delta_j n_j + \delta_{j+1}n_{j+1})} + \cdots + d_s p^{-(\delta_j n_j + \cdots + \delta_s n_s)} \colon n_1, \ldots, n_s \geq 0\}\end{aligned}$$

then we have $S = \{d_{j-1}\} + S_1 + S_2$ where S_1 is the set

$$\left\{c_0 + c_1 p^{\delta_{j-1}n_{j-1}} + c_2 p^{\delta_{j-1}n_{j-1}+\delta_{j-2}n_{j-2}} \cdots + c_{j-1}p^{\delta_{j-1}n_{j-1}+\cdots+\delta_1 n_1} \colon n_1, \ldots, n_{j-1} \geq 0\right\}$$

and S_2 is the set

$$\left\{d_j p^{-\delta_j n_j} + d_{j+1}p^{-(\delta_j n_j + \delta_{j+1}n_{j+1})} + \cdots + d_s p^{-(\delta_j n_j + \cdots + \delta_s n_s)} \colon n_j, \ldots, n_s \geq 0\right\}.$$

Then $G(t) := \sum_{\alpha \in S} t^\alpha$ can be written as a product $t^{d_{j-1}}G_1(t)G_2(t)$, where $G_i(t) = \sum_{\alpha \in S_i} t^\alpha$ for $i = 1, 2$. Then from the above we have $G_1(t) \in C \subseteq \widetilde{C}$ and since $S_2 \subseteq (-\infty, 0)$, a variant of the above argument used with negative powers of p and applying Lemma 87 gives that $G_2(t) \in \widetilde{C}$ and so $G(t) \in \widetilde{C}$. □

Proof of Theorem 3 (a) and the equality $\widetilde{A} = \widetilde{C}$ in Theorem 85. Proposition 82 gives $C \subseteq A$ and $\widetilde{C} \subseteq \widetilde{A}$. We want to show that $A \subseteq C$ and $\widetilde{A} \subseteq \widetilde{C}$. We first show $A \subseteq C$. Let $G(t) = \sum_{n=0}^{\infty} g(n)t^n \in \bar{\mathbb{F}}_p[[t]]$ be an algebraic power series with sparse support. Since $G(t)$ is algebraic, there exists a power q of p such that $G(t) \in \mathbb{F}_q[[t]]$ by Theorem 48. For $\alpha \in \mathbb{F}_q^*$, we define $S_\alpha := \{n \in \mathbb{N} \colon g(n) = \alpha\} \subseteq \mathbb{N}$. By assumption, S_α is sparse for each nonzero α in $\mathbb{F}_q$. Then we can write

$$G(t) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha \left(\sum_{n \in S_\alpha} t^n\right).$$

Since each S_α is sparse, by Equation (2.5), each S_α admits a decomposition into disjoint sets

$$\bigsqcup_{i=1}^{d_\alpha} S_{\alpha,i}$$

for some integer $d_\alpha \geq 1$ with each $S_{\alpha,i}$ a simple sparse set. For $\alpha \in \mathbb{F}_q$ and $i = 1, \ldots, d_\alpha$, we define

$$G_{S_{\alpha,i}}(t) := \sum_{n \in S_{\alpha,i}} t^n.$$

Then we have

$$G(t) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha \left(\sum_{i=1}^{d_\alpha} G_{S_{\alpha,i}}(t) \right).$$

Now by Lemma 88, each $G_{S_{\alpha,i}}(t)$ is in C and so $G(t)$ is also in C. Therefore it follows that $A \subseteq C$. Now, similarly for $\widetilde{A} \subseteq \widetilde{C}$, let $H(t) = \sum_{s \in S} h(s)t^s \in \bar{\mathbb{F}}_p((t^{\mathbb{Q}}))$ be an algebraic generalized Laurent series with sparse support. Since $H(t)$ is algebraic, there exists a power q of p such that $H(t) \in \mathbb{F}_q((t^{\mathbb{Q}}))$ by Theorem 48. For $\alpha \in \mathbb{F}_q^*$, we define $S_\alpha := \{s \in \mathbb{Q} \colon h(s) = \alpha\} \subseteq \mathbb{Q}$. By assumption, S_α is sparse for each nonzero α in $\mathbb{F}_q$. Then we can write

$$H(t) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha \left(\sum_{s \in S_\alpha} t^s \right).$$

Since each S_α is sparse, by Equation (2.5), each S_α admits a decomposition into disjoint sets

$$\bigsqcup_{i=1}^{d_\alpha} S_{\alpha,i}$$

for some integer $d_\alpha \geq 1$ with each $S_{\alpha,i}$ a simple sparse set. For $\alpha \in \mathbb{F}_q$ and $i = 1, \ldots, d_\alpha$, we define

$$H_{S_{\alpha,i}}(t) := \sum_{s \in S_{\alpha,i}} t^s.$$

Then we have

$$H(t) = \sum_{\alpha \in \mathbb{F}_q^*} \alpha \left(\sum_{i=1}^{d_\alpha} H_{S_{\alpha,i}}(t) \right).$$

Now by Lemma 88, each $H_{S_{\alpha,i}}(t)$ is in $\tilde{C}$ and so $H(t)$ is also in $\tilde{C}$. The result follows. □

We now prove Theorem 3 (b), which in terms of Notation 84 can be expressed as $A = B \cap \bar{\mathbb{F}}_p[[t]]$. In order to prove this equality, we must first obtain a description of L_0, which appears in the definition of B.

To give a better picture of L_0, it is necessary to first know all valuations of K. We recall that the places of the field $\bar{\mathbb{F}}_p(t)$ that are constant on $\bar{\mathbb{F}}_p$ are parametrized by the projective line over $\bar{\mathbb{F}}_p$ (see Zariski-Samuel [48, Ch. VI, §17]). Since valuations of $\bar{\mathbb{F}}_p$ are all trivial, these are in fact all places. Each such place is a discrete valuation of $\bar{\mathbb{F}}_p(t)$ and for $\lambda \in \mathbb{P}^1 \setminus \{0, \infty\}$ these valuations lift uniquely to a valuation of K with the same value group as its restriction to $\bar{\mathbb{F}}_p(t)$; that is, K is an extension of $\bar{\mathbb{F}}_p(t)$ that is unramified outside of 0 and ∞. If we had included p-th power roots of t in our definition of K, the value groups of the extensions of these valuations would necessarily increase from $\mathbb{Z}$ to $\mathbb{Z}[1/p]$.

We begin with a simple result characterizing integral closure in terms of valuations that we shall use in the proof of the main theorem.

Lemma 89. *Adopt the notation of Notation 84 and let E be a finite Galois extension of K. Then $a \in \mathcal{V}_{E,+}$ if and only if a is integral over R.*

Proof. Let $\mathcal{X}$ denote the set of valuations on E whose restriction to K is of the form ν_λ for some $\lambda \in \bar{\mathbb{F}}_p^*$. First suppose that $a \in E$ is integral over R. Then a satisfies a non-trivial polynomial equation $a^n + r_{n-1}a^{n-1} + \cdots + r_0 = 0$ for some $n \geq 1$ and $r_0, \ldots, r_{n-1} \in R$. Then if μ is a valuation of E with $\mu|_K = \nu_\lambda$ for some $\lambda \in \bar{\mathbb{F}}_p^*$ and $\nu(r_i) \geq 0$ for $i = 0, \ldots, n-1$. Then if $\nu(a) < 0$ for some $\nu \in \mathcal{X}$, we necessarily have $\nu(a^n) = n\nu(a) < i\nu(a) \leq \nu(r_i a^i)$ for $i = 0, \ldots, n-1$, which contradicts the fact that $a^n = -(r_{n-1}a^{n-1} + \cdots + r_0)$. Thus $a \in \mathcal{V}_{E,+}$. Conversely, suppose that $a \in \mathcal{V}_{E,+}$ and that a is not integral over R. Then since a is not integral over R and a is necessarily nonzero we have a is not integral over $R[a^{-1}]$ since otherwise, we would have a non-trivial polynomial relation of the form $0 = a^n + p_{n-1}(a^{-1})a^{n-1} + \cdots + p_0(a^{-1})$, with each $p_i(a^{-1}) \in R[a^{-1}]$, and then multiplying by a sufficiently large power of a would give that a is integral over R. In particular, a^{-1} is not a unit of the integral closure S of $R[a^{-1}]$ and so there is a height one prime Q of S such that $a^{-1} \in Q$. Then the local ring S_Q is a discrete valuation ring and the valuation ν on E induced by Q gives a rank-one discrete valuation of K corresponding to the valuation induced by the prime ideal $R \cap Q$ of R. In particular, there is some $\lambda \in \bar{\mathbb{F}}_p^*$ such that $\nu|_K$ is equivalent to ν_λ. Now by construction $a^{-1} \in Q$ and so $\nu(a^{-1}) > 0$ and thus $\nu(a) < 0$, which contradicts the fact that $a \in \mathcal{V}_{E,+}$. □

Lemma 90. *Adopt the notation from Notation 84, let E be a finite extension of K, let $\lambda \in \bar{\mathbb{F}}_p^*$, and let $\mathcal{Y}$ be the set of valuations of E whose restriction to K is equal to ν_λ. Then for each $\mu \in \mathcal{Y}$, there exists $\epsilon \in \mathcal{V}_{E,+}$ such that $\mu'(\epsilon - \delta_{\mu,\mu'}) > 0$ for all $\mu' \in \mathcal{Y}$.*

Proof. Let T denote the integral closure of R in E. Then $P := \{r \in R \colon \nu_\lambda(r) > 0\}$ is a maximal ideal of R. Let $Q_1, \ldots, Q_s$ denote the prime ideals of T that lie above R. Then each local ring T_{Q_i} is a discrete valuation ring and each $\mu \in Y$ is induced by one of these valuation rings. Since the Q_i are maximal ideals, they are in particular pairwise comaximal, and so we see by the Chinese remainder theorem there exists some $\epsilon_i \in T$ such that $\epsilon_i - \delta_{i,j} \in Q_j$. The fact that each $\epsilon_i \in \mathcal{V}_{E,+}$ follows from Lemma 89. The result follows. □

Lemma 91. *Adopt the notation from Notation 84, let E be a Galois extension of K of degree p^m for some $m \geq 0$ that is unramified outside of 0 and ∞, and let a be a nonzero element of E. Then there is some $b \in E$ such that $a - (b^p - b)$ is in $\mathcal{V}_E$.*

Proof. Let $\mathcal{X}$ denote the set of valuations on E whose restriction to K is of the form ν_λ for some $\lambda \in \bar{\mathbb{F}}_p^*$. Then there are finitely many $\mu \in \mathcal{X}$ such that $\mu(a) < 0$. Since E is an extension of K that is unramified outside of 0 and ∞, the value group of each $\mu \in \mathcal{X}$ is the same as the value group of the corresponding ν_λ and so $(t - \lambda)$ is a uniformizing parameter for the valuation ring of μ. Let $\mu_1, \ldots, \mu_d$ be the finite set of valuations in $\mathcal{X}$ for which $\mu_i(a) \in \{-p, -2p, \ldots\}$ for $i \in \{1, \ldots, d\}$, and let $m_1, \ldots, m_d$ be the positive integers such that $\mu_i(a) = -pm_i$.

Let $M = M(a) := m_1 + \cdots + m_d$. We prove the claim by induction on M. When $M = 0$ (i.e., $d = 0$), there is nothing to show. We next assume that the claim holds whenever $M < N$ and we consider the case when $M = m_1 + \cdots + m_d = N$. Let $\lambda \in \bar{\mathbb{F}}_p^*$ be such that $\mu_1|_K = \nu_\lambda$. Then since $\mu_1(a) = -m_1 p$, there is some $c \in \bar{\mathbb{F}}_p^*$ such that $\mu_1(a - c^p/(t-\lambda)^{m_1 p}) > \mu_1(a)$. By Lemma 90, there is some $\epsilon \in \mathcal{V}_{E,+}$ such that $\mu(\epsilon - \delta_{\mu,\mu_1}) > 0$ for all valuations $\mu \in \mathcal{X}$ with $\mu|_K = \mu_1|_K$. It follows that for a sufficiently large $s > 1$ we have $\mu(a - c^p\epsilon^{p^s}/(t-\lambda)^{m_1 p} + c\epsilon^{p^{s-1}}/(t-\lambda)^{m_1}) = \mu(a)$ for $\mu \in \mathcal{X}$ and $\mu \neq \mu_1$ and $\mu_1(a - c^p\epsilon^{p^s}/(t-\lambda)^{m_1 p} + c\epsilon^{p^{s-1}}/(t-\lambda)^{m_1}) < \mu_1(a)$. Letting $a' = a - c^p\epsilon^{p^s}/(t-\lambda)^{m_1 p} + c\epsilon^{p^{s-1}}/(t-\lambda)^{m_1}$ and noting that $\epsilon \in \mathcal{V}_{E,+}$, we see that $M(a') < M(a)$. Then by the induction hypothesis there is some $b \in E$ such that $a' - b^p + b \in \mathcal{V}_E$ and so $a - (b')^p + b' \in \mathcal{V}_E$ with

$$b' = b + c\epsilon^{p^{s-1}}/(t-\lambda)^{m_1}.$$

The result follows. □

Lemma 92. *Adopt the notation of Notation 84. Then $\widetilde{C} \subseteq B$ and $C \subseteq B \cap \bar{\mathbb{F}}_p[[t]]$.*

Proof. By the definitions of $\widetilde{C}$ and C it suffices to show that B is Artin-Schreier closed in the ring of generalized Laurent series and that $B \cap \bar{\mathbb{F}}_p[[t]]$ is Artin-Schreier closed in the ring of formal power series over $\bar{\mathbb{F}}_p$, since B contains R.

Since the substitutions $t \mapsto \alpha t$ with $\alpha \in \bar{\mathbb{F}}_p^*$ preserve $\mathbb{P}^1 \setminus \{0, \infty\}$, B and $B \cap \bar{\mathbb{F}}_p[[t]]$ both have property (P2) in Definition 79. Similarly, since for c a nonzero rational number with p-adic valuation 1, the map $t \mapsto t^c$ induces an automorphism of R; moreover, if $c > 0$ then this extends to an automorphism of the ring of generalized Laurent series. Thus if $F(t) \in B$ then $F(t^c) \in B$ and if $F(t) \in B \cap \bar{\mathbb{F}}_p[[t]]$ and $F(t^c) \in \bar{\mathbb{F}}_p[[t]]$ then $F(t^c) \in B \cap \bar{\mathbb{F}}_p[[t]]$. By construction, B is closed under the maps induced by $t \mapsto t^p$ and $t \mapsto t^{1/p}$ and so we then see property (P3) holds in both cases.

Thus it remains to verify that property (P1) holds. Suppose that $F(t) \in B$. Then there is some $j \geq 0$ such that $G(t) := F(t^{p^j})$ is in L_0 and is integral over R. Let $H(t)$ be a generalized Laurent series that is a solution to $X^p - X = G(t)$. Since $G(t)$ is integral over R, $H(t)$ is integral over R. Let E denote an extension of K containing G that is unramified outside of 0 and ∞. Since $G(t)$ is integral over R, we have $G \in \mathcal{V}_{E,+}$ by Lemma 89. Let ν be valuation of E whose restriction to K corresponds to ν_λ with $\lambda \in \bar{\mathbb{F}}_p$. Then since E is an extension of K that is unramified outside of 0 and ∞, and $\nu(G) \geq 0$, we can complete with respect to the valuation ν and we see that G has a formal power series expansion in the variable $u = t - \lambda$. Write $G(u) = \sum_{i \geq 0} a_i u^i$ and let $G_+(u) = \sum_{i \geq 1} a_i u^i$. Then $H_1(u) := G_+(u) + G_+(u^p) + \cdots$ is a power series in u and since H is a solution to $X^p - X = G$, H is of the form $H_1 + \beta$ for some $\beta \in \bar{\mathbb{F}}_p$ with $\beta^p - \beta = a_0$. In particular, H lies in the completion of the valuation ring of ν and so the value groups of the extensions of ν to $E(H)$ are all equal to the value group of ν (more precisely u is a uniformizing parameter for the valuation ring of $E(H)$ for each valuation above ν) and so $E(H)$ is unramified at all extensions of ν to $E(H)$. Thus the field $E(H)$ is an extension of K that is unramified outside of 0 and ∞ and so $H \in B$. Thus B has properties (P1)–(P3) and the result follows. □

Proof of Theorem 3 (b) and the equality $B = \widetilde{A}$ in Theorem 85. We adopt the notation of Notation 84. Suppose that $G(t) \in B$. We shall first show that $G(t)$ is sparse. We may replace $G(t)$ by $G(t^{p^j})$ and assume that $G \in L_0$. Let E denote the Galois closure of $G(t)$ over K. Then $[E : K] = p^m$ for some $m \geq 0$. We prove this by induction on m. If $m = 0$, $G \in K$ and since G is integral over R and R is integrally closed in K, $G \in R$, and so G is easily seen to be sparse in this case, as elements of R have finite support. Now we suppose that the result holds whenever $m < s$ with $s \geq 1$ and we consider the case when $m = s$.

By Remark 61, there is a Galois extension E_0 of K of degree p^{s-1} that is unramified outside of 0 and ∞ with $E = E_0[H]$ and $H^p - H = F \in E_0$. By Lemma 91, there is some $b \in E_0$ such that $F - b^p + b \in \mathcal{V}_{E_0}$. Thus after replacing H by $H + b$, we may assume that $F \in \mathcal{V}_{E_0}$. Then notice in fact that we must have $F \in \mathcal{V}_{E_0,+}$ since otherwise there would be some valuation ν of E_0 with $\nu(F) < 0$ and $p \nmid \nu(F)$. Then since $H^p - H = F$, we have

$\nu'(H) = \nu(F)/p \notin \mathbb{Z}$ for every extension ν' of ν to E. In particular, this contradicts the fact that E is unramified outside of 0 and ∞. Thus F is integral over R by Lemma 89 and so $F \in B$ and thus F is sparse by the induction hypothesis. Hence H is a sparse generalized power series by Proposition 82. Moreover, $H \in B$ as E is unramified over K outside of 0 and ∞ and H is integral over R since F is integral over R. Then since $G(t) \in E_0[H]$, we can write $G = e_0 + e_1 H + \cdots + e_{p-1}H^{p-1}$ with $e_0, \ldots, e_{p-1} \in E_0$. We claim that $e_0, \ldots, e_{p-1} \in B$. To see this, suppose that this is not the case. Then there is some largest $i \geq 0$ for which $e_i \notin B$. Then $G_0 = e_0 + e_1 H + \cdots + e_i H^i \in B$, since $G \in H$ and $e_j H^j \in B$ for $j > i$. Since E is a Galois extension of E_0 and $H^p - H \in E_0$, there is an automorphism of E that fixes E_0 element-wise and sends H to $H + 1$. Since σ fixes K element-wise, σ preserves elements of B. In particular, the operator $\Delta : E \to E$ given by $\Delta(a) = \sigma(a) - a$ maps elements of $B \cap E$ to elements of $B \cap E$. Notice that

$$\Delta^i(G_0) = i!e_i \notin B,$$

which is a contradiction since $G_0 \in B$ and B is preserved under application of Δ. Thus $e_0, \ldots, e_{p-1} \in B$. By the induction hypothesis, $e_0, \ldots, e_{p-1}$ are sparse generalized power series and since H is also a sparse generalized power series, G must be too, since sparse series form a ring. The result now follows by induction. Hence $G(t) \in \widetilde{A}$. By Lemma 92 and the fact that $\widetilde{A} = \widetilde{C}$, established earlier, we see that $\widetilde{A} = \widetilde{C} \subseteq B$ and so $B = \widetilde{A}$. It is straightforward to show that $\widetilde{A} \cap \bar{\mathbb{F}}_p[[t]] = A$ and so we also get $B \cap \bar{\mathbb{F}}_p[[t]] = A$. This completes the proof. □

Chapter 7

Future directions

We have seen that many important results about automatic sets have natural refinements when one restricts one's focus to those automatic sets that are sparse. In fact, for any result about automatic sets, we believe one should also consider as a follow-up question what happens in the sparse case. With this point of view, there is then no shortage of interesting questions about sparse automatic sets. For example, a sparse version of Cobham's theorem is provided in Chapter 4 and also an evidence is presented towards the following conjecture.

Conjecture 93. *(Bell, 2020) Let k and ℓ be multiplicatively independent positive integers. If S is a sparse k-automatic set and T is a zero density ℓ-automatic set, then $S \cap T$ is finite.*

But one area of focus that we feel might be of potential interest is to define a notion of a sparse regular series instead of sparse automatic ones. We saw earlier that k-regular sequences, first defined by Allouche and Shallit [3, 4], are a natural generalization of k-automatic sequences. Many of the fundamental results in automata theory have been extended to the case of regular sequences, including, in particular, Cobham's big theorem [7].

It is not immediately clear what the correct notion of sparseness should be in the context of regular sequences; a naive possibility would be to look at the set of values n for which $f(n) \neq 0$ and insist that this be a sparse automatic set. While we do not currently know what the correct analogue for sparseness should be in this context, we feel that finding the right definition and then considering similar refinements as we have for results about regular sequences would be a worthwhile subject of study.

Bibliography

[1] S. Albayrak and J. P. Bell, A Refinement of Christol's Theorem. Available online at arXiv:1909.02942, 2019.

[2] J.-P. Allouche and J. Shallit, Automatic Sequences. Theory, applications, generalizations. *Cambridge University Press, Cambridge*, 2003.

[3] J.-P. Allouche and J. Shallit, The ring of k-regular sequences. *Theoret. Comput. Sci.* **98** (1992), no. 2, 163–197.

[4] J.-P. Allouche and J. Shallit, The ring of k-regular sequences. II. *Theoret. Comput. Sci.* **307** (2003), no. 1, 3–29.

[5] N. Alon, Combinatorial Nullstellensatz. Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comput.* **8** (1999), no. 1-2, 7–29.

[6] J. P. Bell, A Gap Result for the Norms of Semigroups of Matrices. *Linear Algebra and its Applications* **402** (2005), 101–110.

[7] J. P. Bell, A generalization of Cobham's theorem for regular sequences. *Sém. Lothar. Combin.* 54A (2005/07), Art. B54Ap. 15 pp.

[8] J. P. Bell, Logarithmic frequency in morphic sequences. *J. Théor. Nombres Bordeaux* **20** (2008), no. 2, 227–241.

[9] J. P. Bell, The upper density of an automatic set is rational. To appear in *J. Théor. Nombres Bordeaux*. Preprint available at arXiv:2002.07256.

[10] J. P. Bell, D. Ghioca, and T. J. Tucker, The Dynamical Mordell–Lang Conjecture. Mathematical Surveys and monographs, 210. *American Mathematical Society, Providence, RI*, 2016.

[11] J. P. Bell, K. Hare, and J. Shallit, When is an automatic set an additive basis? *Proc. Amer. Math. Soc. Ser. B* **5** (2018), 50–63.

[12] J. P. Bell and R. Moosa, F-sets and Finite automata. *J. Théor. Nombres Bordeaux* 31 (2019), no. 1, 101–130.

[13] N. Chomsky and M. P. Schützenberger, *The algebraic theory of context-free languages.* Computer programming and formal systems pp. 118–161, North-Holland, Amsterdam, 1963.

[14] G. Christol, Ensembles presque periodiques k-reconnaissables. *Theoret. Comput. Sci.* **9** (1979), 141–145.

[15] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, Suites algébriques, automates et substitutions. *Bull. Soc. Math. France* **108** (1980), 401–419.

[16] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory* **3** (1969), 186–192.

[17] A. Cobham, Uniform tag sequences. *Math Systems Theory* **6** (1972), 164–192.

[18] H. Derksen, A Skolem-Mahler-Lech theorem in positive characteristic and finite automata. *Invent. Math.* **168** (2007), no. 1. 175–224.

[19] P. Erdős and P. Turán, On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* **16** (1941), no. 4. 212–216.

[20] J.-H. Evertse, On sums of S-units and linear recurrences. *Compos. Math.* **53** (1984), 225–244.

[21] J.-H. Evertse and K. Győry, Unit equations in Diophantine number theory. *Cambridge Studies in Advanced Mathematics*, 146. Cambridge University Press, Cambridge, 2015.

[22] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group. *Ann. of Math.* **155** (2002), 807–836.

[23] P. Gawrychowski, D. Krieger, N. Rampersad, and J. Shallit, Finding the growth rate of a regular or context-free language in polynomial time. *Int. J. Found. Comput. Sci.* **21** (2010), 597–618.

[24] D. Ghioca, The isotrivial case in the Mordell-Lang theorem. *Trans. Amer. Math. Soc.* **360** (2008), no. 7, 3839–3856.

[25] S. Ginsburg and E. Spanier, Bounded regular sets. *Proc. Amer. Math. Soc.* **17** (1966), 1043–1049.

[26] H. Hahn, Über die nichtarchimedischen Größensysteme (1907). Gesammelte Abhandlungen I, Springer-Verlag, 1995.

[27] O. H. Ibarra and B. Ravikumar, On sparseness, ambiguity, and other decision problems for acceptors and transducers. *STACS 86 (Orsay, 1986)*, 171–179, *Lecture Notes in Comput. Sci.*, **210**, *Springer, Berlin*, 1986.

[28] K. S. Kedlaya, Finite automata and algebraic extensions of function fields. *J. Théor. Nombres Bordeaux* **18** (2006), no. 2, 379–420.

[29] K. S. Kedlaya, On the algebraicity of generalized power series. *Beitr. Algebra Geom.* **58** (2017), no. 3, 499–527.

[30] S. C. Kleene, Representation of events in nerve nets and finite automata. *Automata Studies*, 3–42. Princeton University Press, 1956.

[31] T. J. P. Krebs, A more reasonable proof of Cobham's theorem. Preprint, available online at arXiv:1801.06704, 2018.

[32] W. Kuo, Y.-R. Liu, and X. Zhao, The asymptotic estimates and Hasse principle for multidimensional Waring's problem. *Adv. Math.* **353** (2019), 1–66.

[33] S. Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, **211**. *Springer-Verlag, New York*, 2002.

[34] M. Lothaire, *Algebraic Combinatorics on Words.* Encyclopedia of Mathematics and its Applications, **90**. *Cambridge University Press, Cambridge*, 2002.

[35] R. Moosa and T. Scanlon, The Mordell-Lang conjecture in positive characteristic revisited. *Model Theory and its applications*, 273–296, Quad. Mat. **11**, *Aracne, Rome*, 2002.

[36] R. Moosa and T. Scanlon, F-structures and integral points on semiabelian varieties over finite fields. *Amer. J. Math.* **126** (3) (2004), 473–522.

[37] M. B. Nathanson, Additive Number Theory: The Classical Bases. *Springer*, 1996.

[38] O. Salon, Suites automatiques à multi-indices et algébricité. *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), no. 12, 501–504.

[39] O. Salon, Suites automatiques à multi-indices (with an appendix by J. Shallit). *Sem. Théorie Nombres Bordeaux* **4** (1986–1987), 1–27.

[40] H. P. Schlickewei, S-unit equations over number fields. *Invent. Math.* **102** (1990), 95–107.

[41] W. M. Schmidt, *Diophantine Approximation.* Lecture Notes in Mathematics, 785. Springer-Verlag Berlin Heidelberg, 1980.

[42] J.-P. Serre, *Local fields.* Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[43] J. Shallit, A. Szilard, S. Yu, and K. Zhang, Characterizing regular languages with polynomial densities. *Mathematical foundations of computer science 1992 (Prague, 1992)*, 494–503, *Lect. Notes in Comput. Sci.*, **629**, *Springer, Berlin*, 1992.

[44] V. I. Trofimov, Growth functions of some classes of languages. *Cybern Syst Anal* **17** (1981), 727–731.

[45] R. C. Vaughan and T. D. Wooley, On Waring's problem: some refinements. *Proc. London Math. Soc. (3)* **63** (1991), no. 1, 35–68.

[46] B. Wei and T. D. Wooley, On sums of powers of almost equal primes. *Proc. Lond. Math. Soc. (3)* **111** (2015), no. 5, 1130–1152.

[47] T. D. Wooley, Large improvements in Waring's problem. *Ann. of Math. (2)* **135** (1992), no. 1, 131–164.

[48] O. Zariski and P. Samuel, Commutative Algebra. Vol. II. Reprint of 1960 edition. Graduate Texts in Mathematics, Vol. 29. *Springer-Verlag, New York-Heidelberg*, 1975.