Asymptotic Recursive Line Complexity Behavior of Polynomial Cellular Automata

UROP+ Final Paper, Summer 2015
Bertrand Stone
Mentor: Mr. Chiheon Kim
Project suggested by Prof. Pavel Etingof
Topic suggested by Prof. Richard Stanley

September 1, 2015

Abstract

Cellular automata are dynamical systems which consist of changing patterns of symbols on a grid. The changes are locally determined, so that the symbol in a given position is determined by the symbols surrounding that position in the previous state. Despite the simplicity of their definition, cellular automata may exhibit large-scale complex behavior. This large-scale complexity arising from simple local behavior is of interest in modeling many complex phenomena, such as biological systems and universal computers. In this paper, we consider one-dimensional additive cellular automata with polynomial transition rules T, and investigate the line complexity sequence $a_T(k)$, which gives the number of accessible blocks of length k for each k. We have previously shown that for transition rules $T(x) = 1 + x + x^n$ ($n \geq 3$) with coefficients taken modulo 2, and for certain sequences s_k which are dependent upon a real number $x \in [1/2, 1]$, the quotient $a_T(s_k)/s_k^2$ converges to a piecewise quadratic function of x. Our development was based on recursive expressions for the line complexity sequence. In this paper, we investigate these recursions for general polynomials with coefficients modulo 2, and determine some characteristics of these polynomials that enable a generalization of some of our previous arguments. In particular, we characterize the polynomials for which certain associated maps are injective – an essential feature of these recursions – and show that some intersections that arise in the derivation of such a recursion stabilize in size for sufficiently large k in the case of general polynomial transition rules. We also view the recursions described above in a more general context, introducing a notion of the *order* of a recursion distinct from the order of the transition rule. We investigate the behavior of the line complexity under powers, and show that the property of "having a recursion of some order" is preserved when the transition rule is raised to a positive integer power.

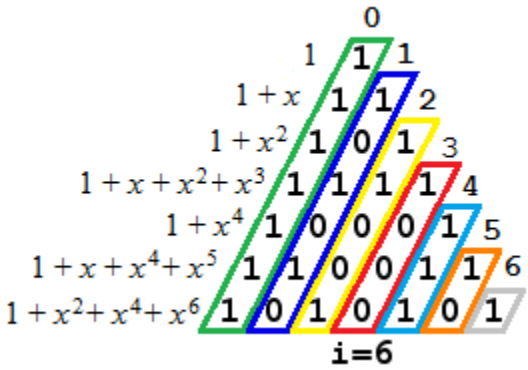

Figure 1: Constructing Pascal's triangle modulo 2

1 Introduction

A *cellular automaton* is a discrete system which consists of patterns of symbols on a grid. These patterns change in successive time intervals, and the changes are specified by a *transition rule*, in such a way that the symbol in a particular location at a particular point in time is determined by the surrounding symbols in the previous state.

In this paper, we shall focus on one-dimensional cellular automata. A particular state for such an automaton is called a *configuration*, and may be expressed as a Laurent series

$$\sum_{-\infty}^{\infty} a_i x^i,$$

where the superscripts correspond to the locations of the values a_i. For example, the expression $x+3x^3+2x^4$ represents the string 01032.

Given a configuration ω, the *transition rule* T for a cellular automaton determines a new configuration $T\omega$ in such a way that the value at a given index i in $T\omega$ is determined by values near i in ω. An *additive* transition rule is specified by a Laurent polynomial and acts upon a configuration by multiplication. In this paper, we will use as an alphabet the integers modulo some prime p. Thus in this case the transition rule acts upon a configuration by multiplication, and the coefficients are reduced modulo p. We illustrate this process by constructing Pascal's triangle modulo 2 in Figure 1; we take $p=2$, $T(x)=1+x$, and start with the initial state $\omega_0=1$.

A more complicated example is obtained by taking $p=2$, $\omega_0=1$, $T(x)=1+x^2+x^4+x^5$. This automaton is illustrated in Figure 2.

Sequences of length k which appear in some configuration are called *k-accessible blocks*. For example, the block 110011 appears in line 5 of the automaton shown in Figure 1, and is thus accessible. We will write $a_T(k)$ for the number of accessible blocks of length k for a given transition rule T (it is implicitly assumed that the initial state has been specified). We define $a_T(0)=1$: the empty string is always accessible. The sequence $a_T(k)$ for $k\geq 0$ is called the *line complexity* of the automaton.

Garbe [1] considered the transition rule $T(x)=1+x$ with coefficients taken modulo general primes p and the rule $T(x)=1+x+x^2$ with coefficients taken modulo small primes p, and investigated the asymptotic behavior of subsequences of the quotient $a_T(k)/k^2$. In [2], we considered the

Figure 2: The automaton obtained by iteratively multiplying $\omega_0 = 1$ by the rule $T(x) = 1 + x^2 + x^4 + x^5$, modulo 2.

case $p = 2$ and investigated the general class of transition rules of the form $T(x) = 1 + x + x^n$, where $n \geq 3$. For certain sequences $s_k(x)$, where $x \in [1/p, 1]$, we showed that $\lim_{k\to\infty} a_T(s_k(x))/s_k(x)^2$ is piecewise quadratic in x. Our argument was based upon iterating an abstract generating function relation of the form

$$\lambda(z)\phi(z) = R(z) + \lambda(z^p)\phi(z^p),$$

where ϕ is a generating function for the line complexity sequence (possibly with shifted coefficients), R is a polynomial with $R(1) = 0$, and λ is the reciprocal of a power series whose coefficients are of the form $\gamma(k) = Ck^2 + f(k)$, with $C > 0$, $f(0) = 1$ and $f(k) = o\left(\frac{k^2}{\log_p x}\right)$. We showed that the asymptotic behavior of $a_T(s_k(x))/s_k(x)^2$ we observed may be derived entirely from these functional relations; we derived these relations, in turn, from recursive expressions for the line complexity sequence of a form which we will describe in Section 3. We proved these relations by an argument involving the inclusion-exclusion principle; one important feature of these recursions is that the size of the intersections is eventually constant.

In this paper, we examine these recursions for general polynomials, and determine some characteristics of these polynomials that enable a generalization of some of our previous arguments. In Section 2, we introduce some useful notation. In Section 3, we will describe the general structure of the recursion relations, and we will see the importance of the injectivity of several transformations that we will introduce. In Section 4, we investigate the injectivity of these maps, and provide a complete characterization of which polynomials induce injective maps on the whole space. In Section 5, we investigate the asymptotic size of some intersections that arise in Section 3. In Section 6, we examine some interesting consequences of introducing a notion of the *order* of a recursion, and characterize the behavior of the line complexity sequence when the transition rule is raised to a power.

2 Notation

In this section, we introduce some notation which we will use throughout the rest of the paper.

In the following, we will write $A_p(I;T)$ for the automaton generated by iteratively multiplying I by T and reducing the coefficients modulo p. We will assume throughout that $I, T \in (\mathbb{Z}/p)[x]$. We will write $\mathscr{A}(k)$ for the set of accessible blocks of length k associated to such an automaton.

We shall write $1^2 01 = 1101$ etc. in block notation; to distinguish this notation from operations such as squaring, we shall write the latter with square brackets, e.g.

$$[(111)^2] = (1 + x + x^2)^2 = 10101,$$

whereas

$$(111)^2 = 111111.$$

If $b = b_0 \cdots b_n$, we will write $b|_{i\cdots j} = b_i \cdots b_j$. At the end of a block, we employ the notation 0_l to represent sufficiently many zeros to bring the total length of the block to $l+1$; for example $1010_5 = 101000$.

If f and g are polynomials, we will write $(f,g) = 1$ to indicate that f and g have no nontrivial common factors.

3 Recursion Formulas for the Line Complexity Sequence

Our study of the asymptotic properties of the line complexity sequence is based upon recursion formulas for $a_T(2k)$ and $a_T(2k+1)$. These recursions hold for sufficiently large k, and their structure is motivated by the following analysis. We shall focus on the recursion for $a_T(2k)$.

Consider an automaton $A_2(1;T)$, where T is a polynomial of degree n, and some even row of this automaton, say $2r$. We see that this line of the automaton is of the form

$$T^{2r}(1) = T^{2r} = (T^r)^2. \tag{1}$$

In view of the identity $T(s^2) \equiv T(s)^2 \pmod 2$, squaring a polynomial has the effect of inserting zeros between the original coefficients; thus (in block notation) we have

$$[(x_0x_1x_2)^2] = x_00x_10x_2.$$

Since line $2r$ of the automaton is a square, we see that all accessible blocks of length $2k$ appearing in this row must be of the form

$$x_00x_10\cdots x_{k-1}0$$

or of the form

$$0x_00x_1\cdots 0x_{k-1}.$$

Moreover, by the identity (1), it follows that $x_0x_1\cdots x_{k-1}$ must be accessible.

We introduce the sets

$$A_1 = \{x_00x_10\cdots x_{k-1}0 : x_0x_1\cdots x_{k-1} \in \mathscr{A}(k)\}$$

and

$$A_2 = \{0x_00x_1\cdots 0x_{k-1} : x_0x_1\cdots x_{k-1} \in \mathscr{A}(k)\},$$

and the maps $T_{A_i} : \mathscr{A}(k) \to A_i$ defined by

$$T_{A_1} : x_0x_1\cdots x_{k-1} \mapsto x_00x_10\cdots x_{k-1}0$$

and

$$T_{A_2} : x_0x_1\cdots x_{k-1} \mapsto 0x_00x_1\cdots 0x_{k-1}.$$

It is clear that the maps T_{A_i} are bijective, so that $|A_1| = |A_2| = a_T(k)$.

The accessible blocks in odd-numbered rows have a more complex structure. We first assume that n is even, and consider a row $2r+1$ of the automaton. We want to establish a correspondence

between accessible blocks of length $2k$ in this row and accessible blocks of some smaller length in row r. We will use the locally-determined nature of the automaton and the fact that all blocks in row $2r+1$ arise by applying the transition rule to row $2r$.

To produce the accessible blocks of length $2k$ in row $2r+1$, we start with a given accessible block b of length $k+\frac{n}{2}$ in line r. It follows that the block $0[b^2]0$ is a block of length $2k+n+1$ which appears in row $2r$. (Moreover, as we saw in the case of the sets A_i, all such blocks are produced in this way.) We now apply the transition rule to this block, obtaining a block of length $2k+2n+1$ in row $2r+1$ (the right side of the block must be padded with zeros to ensure this). We now eliminate the n entries on either side of the resulting block, obtaining a block of length $2k+1$. This is necessary because in the context of the entire automaton, the block b does not determine these n entries on either side. This leaves a block t of length $2k+1$. Finally, define

$$T_{B_1} b = t_0 \cdots t_{2k-1}$$

and

$$T_{B_2} b = t_1 \cdots t_{2k}.$$

Briefly, we can write

$$T_{B_i} b = T\left(0[b^2]0\right) 0_{2k+2n}|_{n+i-1 \cdots n+2k+i-1}.$$

For example, consider the automaton $A_2(1, 1+x+x^2)$. We outline the above process in the following schematic:

$$\begin{array}{ll} b & 1011 \\ 0[b^2]0 & 010001010 \\ & \overbrace{}^{T_{B_2} b} \\ T(0[b^2]0)0_{2k+2n} & 01|\underbrace{1101101}_{T_{B_1} b}|10 \end{array}$$

In the above example, we note that if there had been a 1 immediately to the left of the block $0[b^2]0$, the two leftmost entries of $T(0[b^2]0)0_{2k+2n}$ would be changed to 10. We thus see that these two entries cannot be determined by b alone; this is why n entries must be deleted on either side of $T(0[b^2]0)0_{2k+2n}$.

We now define

$$B_1 = T_{B_1}\left(\mathscr{A}(k+\tfrac{n}{2})\right)$$

and

$$B_2 = T_{B_2}\left(\mathscr{A}(k+\tfrac{n}{2})\right).$$

Thus the maps $T_{B_i} : \mathscr{A}(k+\frac{n}{2}) \to B_i$ are clearly surjective.

The case of odd n is similar, but with some modification. Namely, in this case, the map T_{B_1} acts upon blocks in $\mathscr{A}(k+\frac{n-1}{2})$, and the map T_{B_2} acts upon blocks in $\mathscr{A}(k+\frac{n+1}{2})$. The sets B_i are defined in an analogous manner.

If we can show that the maps T_{B_i} are *injective* as well, by the inclusion-exclusion principle we arrive at the following general recursion:

$$\begin{aligned} a_T(2k) = {} & 2a_T(k) + a_T(k + \lfloor \tfrac{n}{2} \rfloor) + a_T(k + \lfloor \tfrac{n+1}{2} \rfloor) \\ & - |A_1 \cap A_2| - |A_1 \cap B_1| - |A_1 \cap B_2| - |A_2 \cap B_1| - |A_2 \cap B_2| - |B_1 \cap B_2| \\ & + |A_1 \cap B_1 \cap B_2| + |A_2 \cap B_1 \cap B_2| + |A_1 \cap A_2 \cap B_1| + |A_1 \cap A_2 \cap B_2| \\ & - |A_1 \cap A_2 \cap B_1 \cap B_2|. \end{aligned}$$

We will investigate the injectivity of the maps T_{B_i} in the next section, and we will examine the intersections in the subsequent section.

4 Injectivity

We will now characterize the polynomials for which the maps T_{B_i} are injective on the whole space; for example, if n is even, we will characterize the polynomials for which the maps

$$T_{B_i} : (\mathbb{Z}/2)^{k+\frac{n}{2}} \to (\mathbb{Z}/2)^{2k}$$

are injective; it follows that the maps

$$T_{B_i} : \mathscr{A}(k + \tfrac{n}{2}) \to B_i$$

are then bijective.

We will express the maps T_{B_i} in matrix form. The rule T can be written explicitly as

$$T(x) = c_0 + c_1 x + \ldots + c_n x^n.$$

If we wish to multiply this polynomial by another polynomial $S(x) = d_0 + d_1 x + \ldots + d_m x^m$, we construct a matrix with $m+1$ columns, of the form

$$M = \begin{bmatrix} c_0 & & & \\ c_1 & c_0 & & \\ \vdots & c_1 & & \\ c_n & \vdots & & c_0 \\ & c_n & \vdots & c_1 \\ & & & \vdots \\ & & & c_n \end{bmatrix}.$$

$(TS)(x)$ is then given by multiplying M by the coefficient vector $(d_0, d_1, \ldots, d_m)$, and expressing the result in the basis $(1, x, x^2, \ldots, x^{n+m})$. Suppose n is even. The action of the map T_{B_1} on a $(k+\frac{n}{2})$-block can be described by the action of a matrix $[T_{B_1}]$ on this block. We obtain the matrix $[T_{B_1}]$ from M by deleting columns $0, 2, 4$, etc., and deleting the first and last n rows of the resulting matrix.

If we define

$$C = \begin{bmatrix} c_{n-1} & c_{n-3} & \cdots & c_1 & 0 \\ c_n & c_{n-2} & \cdots & c_2 & c_0 \end{bmatrix},$$

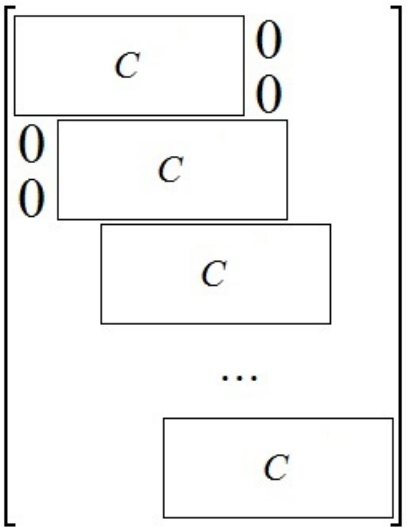

Figure 3: The matrix $[T_{B_1}]$

we see that $[T_{B_1}]$ is the $2k \times (k+\frac{n}{2})$ matrix in Figure 3.

If n is odd, the form of the matrix is also given by Figure 3, but in this case we have

$$C = \begin{bmatrix} c_{n-1} & c_{n-3} & \cdots & c_0 \\ c_n & c_{n-2} & \cdots & c_1 \end{bmatrix}.$$

The matrix for T_{B_1} of shape $2k \times (k+\lfloor \frac{n}{2} \rfloor)$. The matrix for T_{B_2} is constructed in an analogous manner, and is of shape $2k \times (k+\lfloor \frac{n+1}{2} \rfloor)$. A chart of the matrices for T_{B_2} is given in Figure 4.

In the following, we assume that $n \geq 1$. We say that a polynomial is *suspicious* if there exists $k \geq \lfloor \frac{n}{2} \rfloor$ for which either T_{B_1} or T_{B_2} is not injective (note that here the domains are $(\mathbb{Z}/2)^{k+\frac{n}{2}}$ in the even case, instead of $\mathscr{A}(k+\frac{n}{2})$).

The reason for the assumption that $k \geq \lfloor \frac{n}{2} \rfloor$ is the following: if $k < \lfloor \frac{n}{2} \rfloor$, we have

$$\text{rank}[T_{B_1}] \leq 2k < k + \left\lfloor \frac{n}{2} \right\rfloor,$$

so that T_{B_1} is definitely not injective.

We write $T(x) = c_0 + c_1 x + \ldots + c_n x^n \ \ (c_n \neq 0)$ as before, and define

$$o(x) = c_{n-1} + c_{n-3}x + \ldots + c_1 x^{\frac{n}{2}-1}$$
$$e(x) = c_n + c_{n-2}x + \ldots + c_0 x^{\frac{n}{2}}$$

if n is even, and

$$o(x) = c_n + c_{n-2}x + \ldots + c_1 x^{\lfloor \frac{n}{2} \rfloor}$$
$$e(x) = c_{n-1} + c_{n-3}x + \ldots + c_0 x^{\lfloor \frac{n}{2} \rfloor}$$

if n is odd. We are now ready to present a characterization of the nonsuspicious polynomials.

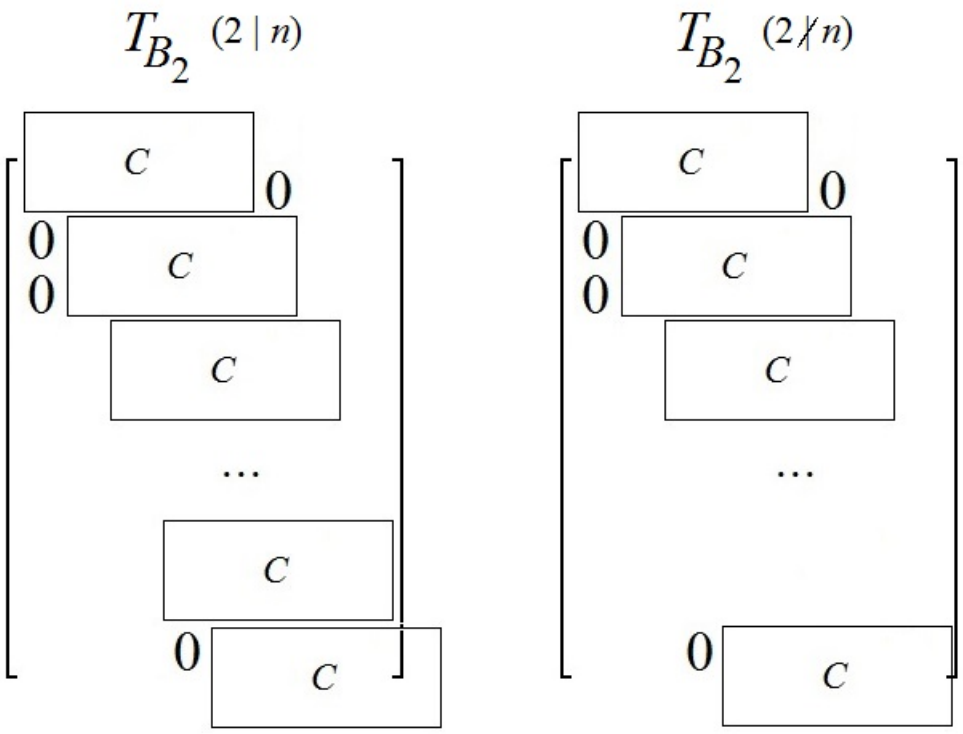

Figure 4: Matrices for the transformation T_{B_2}.

Theorem 1. *If n is even, then*

i. *T_{B_1} is injective if and only if $c_0 \neq 0$ and $(o,e) = 1$, and*

ii. *T_{B_2} is injective if and only if $(o,e) = 1$.*

If n is odd, then

iii. *T_{B_1} is injective if and only if $(o,e) = 1$, and*

iv. *T_{B_2} is injective if and only if $c_0 \neq 0$ and $(o,e) = 1$.*

Corollary 1. *T is nonsuspicious if and only if $c_0 \neq 0$ and $(o,e) = 1$.*

Proof. Consider the map T_{B_1}, and assume that n is even. We claim that for any $k \geq \frac{n}{2}$, T_{B_1} is injective if and only if T_{B_1} is injective in the special case of $k = \frac{n}{2}$. Sufficiency is clear; necessity follows from the structure of the matrix $[T_{B_1}]$, as in the following: we will write $T_{B_1}[k = \frac{n}{2}]$ for the operator T_{B_1} in the case where $k = \frac{n}{2}$.

Suppose

$$T_{B_1} x = 0,$$

where $x = x_0 x_1 \cdots x_{k+\frac{n}{2}-1} \in (\mathbb{Z}/2)^{k+\frac{n}{2}}$. Since the submatrix which consists of the first n rows and columns of T_{B_1} is precisely $[T_{B_1}][k = \frac{n}{2}]$, we see that

$$x_0 = x_1 = \cdots = x_{n-1} = 0.$$

We now observe that the submatrix which consists of the entries in rows 2 through $n+1$ and columns 1 through n is *also* precisely $[T_{B_1}][k = \frac{n}{2}]$, so that

$$x_2 = \cdots = x_n = x_{n+1} = 0.$$

Continuing this process, we conclude that $x = 0$, so that T_{B_1} is injective.

We have shown that it is sufficient to analyze the case of $T_{B_1}[k = \frac{n}{2}]$. We now take the determinant of $[T_{B_1}][k = \frac{n}{2}]$.

We use the fact that the determinant changes only in sign under row permutations. Thus,

$$\det[T_{B_1}][k=\tfrac{n}{2}] = \pm\det\begin{bmatrix} c_{n-1} & c_{n-3} & \cdots & c_1 & & & & \\ & c_{n-1} & c_{n-3} & \cdots & c_1 & & & \\ & & & & \cdots & & & \\ & & & c_{n-1} & c_{n-3} & \cdots & c_1 & 0 \\ c_n & c_{n-2} & \cdots & c_0 & & & & \\ & c_n & c_{n-2} & \cdots & c_0 & & & \\ & & & & \cdots & & & \\ & & & & c_n & c_{n-2} & \cdots & c_0 \end{bmatrix}.$$

By expansion along the last column, we conclude that

$$\det[T_{B_1}][k=\tfrac{n}{2}] = \pm c_0\det\begin{bmatrix} c_{n-1} & c_{n-3} & \cdots & c_1 & & & \\ & c_{n-1} & c_{n-3} & \cdots & c_1 & & \\ & & & & \cdots & & \\ & & & c_{n-1} & c_{n-3} & \cdots & c_1 \\ c_n & c_{n-2} & \cdots & c_0 & & & \\ & c_n & c_{n-2} & \cdots & c_0 & & \\ & & & & \cdots & & \\ & & & c_n & c_{n-2} & \cdots & c_0 \end{bmatrix}.$$

The latter determinant is precisely the *resultant* of the polynomials o and e defined above. By Corollary 1.8 in [3], the resultant of o and e is nonzero if and only if $(o,e) = 1$. We have thus proved part i.

The proofs of the other assertions are similar; to prove part ii we use expansion in the first column; the proof of part iii only requires interchanging rows, and to prove part iv we use expansion in the first and last columns successively. □

5 Intersections

In this section, we investigate the sizes of intersections of the sets A_1, A_2, B_1, and B_2. We will consider the case where the elements are of even length, for specificity. We first note that the only element of $A_1 \cap A_2$ is the zero string 0^{2k}. It follows that

Proposition 1. *We have*

$$|A_1 \cap A_2| = |A_1 \cap A_2 \cap B_1| = |A_1 \cap A_2 \cap B_2| = |A_1 \cap A_2 \cap B_1 \cap B_2| = 1.$$

We now turn to the intersection $B_1 \cap B_2$.

Theorem 2. *If T is a general polynomial in $(\mathbb{Z}/2)[x]$, of degree n, we have*

$$|B_1 \cap B_2| \leq a_T(n) \tag{2}$$

and the size of $B_1 \cap B_2$ is independent of k for sufficiently large k.

Proof. The proof of (2) will be based upon the following observation: *All blocks in $B_1 \cap B_2$ are in the kernel of the transformation*

$$S = \begin{bmatrix} c_n & c_{n-1} & c_{n-2} & & \\ & c_n & c_{n-1} & & \\ & & c_n & & \\ & & & \ddots & \\ & & & & c_0 \end{bmatrix}.$$

To see this, suppose $b = b_0 b_1 \cdots b_{2k-1} \in B_1 \cap B_2$. We assume for specificity that n is even. Since $b \in B_1$, we have $b = T_{B_1} x$ for some $x \in \mathscr{A}(k + \frac{n}{2})$. Consider the product ST_{B_1}. A direct computation shows that the matrix $[ST_{B_1}]$ is given by

$$\begin{bmatrix} c_n & c_{n-1} & \cdots & c_0 & & & \\ & c_n & c_{n-1} & \cdots & c_0 & & \\ & & c_n & c_{n-1} & \cdots & c_0 & \\ & & & & & \cdots & \\ & & & & c_n & c_{n-1} & \cdots & c_0 \end{bmatrix} \begin{bmatrix} c_{n-1} & c_{n-3} & \cdots & c_1 & 0 & & \\ c_n & c_{n-2} & \cdots & c_2 & c_0 & & \\ & c_{n-1} & c_{n-3} & \cdots & c_1 & 0 & \\ & c_n & c_{n-2} & \cdots & c_2 & c_0 & \\ & & & & \cdots & & \\ & & & & \cdots & & \\ & & & c_{n-1} & c_{n-3} & \cdots & c_1 & 0 \\ & & & c_n & c_{n-2} & \cdots & c_2 & c_0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & \cdots & & & & & & \\ c_n^2 & c_{n-1}^2 & \cdots & c_0^2 & 0 & \cdots & & 0 \\ 0 & \cdots & & & & & & \\ 0 & c_n^2 & c_{n-1}^2 & \cdots & c_0^2 & 0 & \cdots & 0 \\ \cdots & & & & & & & \\ 0 & \cdots & & 0 & c_n^2 & c_{n-1}^2 & \cdots & c_0^2 \end{bmatrix} = \begin{bmatrix} 0 & \cdots & & & & & & \\ c_n & c_{n-1} & \cdots & c_0 & 0 & \cdots & & 0 \\ 0 & \cdots & & & & & & \\ 0 & c_n & c_{n-1} & \cdots & c_0 & 0 & \cdots & 0 \\ \cdots & & & & & & & \\ 0 & \cdots & & 0 & c_n & c_{n-1} & \cdots & c_0 \end{bmatrix}.$$

It follows that the ith coordinate of $ST_{B_1}x$ is 0 if $i = 0, 2, \ldots$ is even.

The situation is precisely analogous for T_{B_2}; in this case we conclude that odd coordinates of $ST_{B_2}y$ are zero for $y \in \mathscr{A}(k + \frac{n}{2})$. It follows that $Sb = 0$, so that $b \in \ker S$.

From this we see that $c_n b_0 + c_{n-1} b_1 + \ldots + c_0 b_n = 0$, $c_n b_1 + c_{n-1} b_2 + \ldots + c_0 b_{n+1} = 0$, etc., so that b_n is determined by b_0, b_1, …, b_{n-1}, b_{n+1} is determined by b_1, b_2, …, b_n, etc. It follows that b is determined entirely by $b_0 b_1 \cdots b_{n-1}$, which is clearly accessible; it follows that

$$|B_1 \cap B_2| \leq a_T(n).$$

We employ similar methods to conclude that the above holds for blocks of odd length. We have thus proved (2).

Suppose $n \leq j < k$. From the above we see that every block in $B_1 \cap B_2$ of length $r \geq n$ is generated by a block of length n. The map that assigns to a block of length k the block of length j with the same generator is injective, so that

$$|(B_1 \cap B_2)(j)| \geq |(B_1 \cap B_2)(k)|.$$

In particular, the sequence $|(B_1 \cap B_2)(k)|$ is nonincreasing for $k \geq n$; since $|(B_1 \cap B_2)(k)| \geq 1$, it follows that the sequence is eventually constant.

□

6 Powers of the Transition Rule

So far, our analysis has been based heavily upon the injectivity of the maps T_{B_i}. It turns out, however, that some suspicious polynomials obey recursions similar to those described above. To examine this phenomenon more closely, we introduce the *order* of a recursion.

Suppose p is prime. We say that the automaton $A_p(I;T)$ *satisfies a recursion of order n* if there exist a constant C and integers n, K such that

$$a_T(k) = \sum_{j=0}^{p-1} \sum_{r=0}^{p-1} a_T\left(\left\lfloor \frac{k+jn+r}{p} \right\rfloor\right) + C$$

for all $k \geq K$.

In the modulo 2 case we considered above, the degree of the polynomial and the order of the recursion were the same; in general this need not be the case.

In this section we will show that if the automaton $A_p(c;T)$ (with a constant initial state) satisfies a recursion of order r, then $A_p(c;T^n)$ satisfies a recursion of order rp^s, where s is the largest integer such that $p^s \mid n$.

We will say that an automaton is *trivial* if its transition rule T has at most one nonzero coefficient. Such rules can only translate the initial state or multiply it by a constant. The following proposition shows that non-trivial automata use the entire alphabet available to them.

Proposition 2. *Suppose p is prime. If the automaton $A_p(I;T)$ is non-trivial, then all the symbols $0, 1, \ldots, p-1$ are accessible; that is, $a_T(1) = p$.*

Proof. Write $T(x) = a_0 + a_1 x + \ldots + a_n x^n$. Since $a_{xT(x)}(k) = a_{T(x)}(k)$ for all k, we may assume that $a_0 \neq 0$. We also suppose (since the automaton is nontrivial) that $a_d \neq 0$ for some $d > 0$; we choose d so as to be minimal. Then the coefficient of x^d in the expansion of T^r is $r a_0^{r-1} a_d$. Since p is prime and $a_0 \neq 0$, we have $a_0^{k(p-1)} \equiv 1 \pmod{p}$ (note that the multiplicative group $(\mathbb{Z}/p)^\times$ of nonzero integers modulo p is cyclic, so a_0 has a finite order which divides $p-1$). Thus, taking $r = k(p-1)+1$, we see that $r a_0^{r-1} a_d = (1+k(p-1)) a_0^{k(p-1)} a_d = (1+k(p-1)) a_d$. Since $(\mathbb{Z}/p)^+$ (the *additive* group of integers modulo p) is of prime order, it is cyclic and is generated by every nonzero element. Since $a_d, p-1 \neq 0$, we see that $\{(1+k(p-1))a_d : k \geq 0\} = (\mathbb{Z}/p)^+$, so that the coefficient of x_d assumes all values in $\mathbb{Z}/p$. This completes the proof. □

Proposition 3. *Suppose p is prime, $c, d \in \mathbb{Z}/p$, and the automaton $A_p(d,T)$ is non-trivial. Then if $b \in \mathscr{A}(k)$, $c \cdot b \in \mathscr{A}(k)$.*

Note: in particular, if we consider the operation of multiplication by a constant as an action of $\mathbb{Z}/p$ on $\mathscr{A}(k)$, then this proposition implies that all orbits of blocks in $\mathscr{A}(k)$ are contained in $\mathscr{A}(k)$: we have

$$(\mathbb{Z}/p)(\mathscr{A}(k)) = \mathscr{A}(k) \qquad (k \geq 1).$$

Proof. Since $A_p(d;T)$ is non-trivial, Proposition 2 shows that $c \cdot d \in \mathscr{A}(1)$. Suppose that $c \cdot d$ appears in line r. We first note that $T^p(s) \equiv T(s^p) \pmod{p}$ for any polynomial s, since p is prime. Thus if $j \geq 1$, line $p^j r$ includes the block $0^j (c \cdot d) 0^j$. The block b appears in some line, say r'. If $j > (\deg T) r'$, then lines $0, 1, \ldots, r'$ of the automaton, multiplied by c, appear in the lines $p^j r, \ldots, p^j r + r'$. In particular, we can take $j = (\deg T) r' + 1$; then $c \cdot b$ appears in row $p^{(\deg T) r' + 1} r + r'$. This completes the proof. □

In the following theorem, we show that taking the transition rule to powers relatively prime to the modulo does not change the collection of accessible blocks.

Theorem 3. *Suppose that p is prime, $(p,n)=1$, $c \in \mathbb{Z}/p$, and suppose that $A_p(c;T)$ is non-trivial. Let $\mathscr{A}_n(k)$ denote the set of accessible blocks of length k associated to $A_p(c;T^n)$. Then for all k, we have*

$$\mathscr{A}_1(k) = \mathscr{A}_n(k),$$

and in particular,

$$a_T(k) = a_{T^n}(k).$$

Proof. Since $a_{xT(x)}(k) = a_{T(x)}(k)$, we will assume that T has a nonzero constant coefficient. We first note that line k of $A_p(c;T^n)$ is the same as line kn of $A_p(c;T)$, since at each stage $A_p(c;T^n)$ applies the transition rule n times. From this it clearly follows that $\mathscr{A}_n(k) \subseteq \mathscr{A}_1(k)$ for all k. To show that $\mathscr{A}_n(k) \supseteq \mathscr{A}_1(k)$, suppose that b is a block of length k in $A_p(c;T)$, appearing on some line r. We will show that b appears on a line $L \equiv 0 \pmod{n}$. This is clear if $r \equiv 0 \pmod{n}$; we will thus assume that $r \not\equiv 0 \pmod{n}$.

As in the proof of Proposition 3, we have $T(s)^p \equiv T(s^p) \pmod{p}$ for any polynomial s. Thus if $j \geq 1$ and $T(x) = t_0 + t_1 x + \ldots + t_n x^n$, line 1 of $A_p(c;T)$ is given by $(c \cdot t_0) \cdots (c \cdot t_n)$, so that line p^j is given by $(c \cdot t_0)0^j(c \cdot t_1)0^j \cdots 0^j(c \cdot t_n)$. Thus, as in the proof of Proposition 3, if $j > nr$, lines $0, \ldots, r$ of the automaton $A_p((c \cdot t_0);T)$ appear in lines $p^j, \ldots, p^j + r$ of $A_p(c;T)$.

Since $(p,n)=1$, we have $p^{\phi(n)} \equiv 1 \pmod{n}$ by the Euler-Fermat theorem. In particular, p is of finite order m. Thus, there exists s_1 such that $p^{s_1 m} \equiv 1 \pmod{n}$ and $s_1 m > rn$, so that $t_0 \cdot b$ appears in line $r + p^{s_1 m}$ and $r + p^{s_1 m} \equiv r+1 \pmod{n}$. If $r+1 \equiv 0 \pmod{n}$, then we have $t_0 \cdot b \in \mathscr{A}_n(k)$.

Otherwise, we repeat the above reasoning with r replaced by $r + p^{s_1 m}$: we know that $t_0 \cdot b$ appears in row $r + p^{s_1 m} + p^j$ if $j > n(r + p^{s_1 m})$. Thus there exists s_2 such that $p^{s_2 m} \equiv 1 \pmod{n}$ and $s_2 m > n(r + p^{s_1 m})$. It follows that $t_0 \cdot b$ appears in row $r + p^{s_1 m} + p^{s_2 m}$, and $r + p^{s_1 m} + p^{s_2 m} \equiv r+2 \pmod{n}$. If $r+2 \equiv 0 \pmod{n}$, then $t_0 \cdot b \in \mathscr{A}_n(k)$; otherwise, we proceed in this manner until $r + i \equiv 0 \pmod{n}$ for some i (Note that at most finitely many steps are necessary).

We have shown that $t_0 \cdot b \in \mathscr{A}_n(k)$. Since $\mathbb{Z}/p$ is a field, t_0 has an inverse. By applying Proposition 3 to the automaton $A_p(c;T^n)$, we see that $t_0^{-1} \cdot (t_0 \cdot b) \in \mathscr{A}_n(k)$. We have shown that $\mathscr{A}_1(k) = \mathscr{A}_n(k)$. The conclusion follows. □

Theorem 4. *Suppose p is prime and $0 \leq r < p$. Then we have*

$$a_{T^p}(pk + r) = (p-r)a_T(k) + ra_T(k+1) + 1 - p$$

for all $k \geq 1$.

Proof. First, suppose that $r \geq 1$. We will use the notation $\mathscr{A}_n$ of Theorem 3. In view of the identity $T(s^p) \equiv T(s)^p \pmod{p}$, we see that the accessible coefficient blocks of length $pk + r$ must belong

to one of the following sets:

$$\begin{aligned}
A_1 &= \{x_0 0^{p-1} x_1 0^{p-1} \cdots x_{k-1} 0^{p-1} x_k 0^{r-1} \quad : x_0 \cdots x_k \in \mathscr{A}_1(k+1)\} \\
A_2 &= \{0 x_0 0^{p-1} x_1 0^{p-1} \cdots x_{k-1} 0^{p-1} x_k 0^{r-2} \quad : x_0 \cdots x_k \in \mathscr{A}_1(k+1)\} \\
&\cdots \\
A_r &= \{0^{r-1} x_0 0^{p-1} x_1 0^{p-1} \cdots x_{k-1} 0^{p-1} x_k \quad : x_0 \cdots x_k \in \mathscr{A}_1(k+1)\} \\
A_{r+1} &= \{0^r x_0 0^{p-1} x_1 0^{p-1} x_2 0^{p-1} \cdots x_{k-1} 0^{p-1} : x_0 \cdots x_{k-1} \in \mathscr{A}_1(k)\} \\
&\cdots \\
A_p &= \{0^{p-1} x_0 0^{p-1} x_1 0^{p-1} x_2 0^{p-1} \cdots x_{k-1} 0^r : x_0 \cdots x_{k-1} \in \mathscr{A}_1(k)\}
\end{aligned}$$

Thus $\mathscr{A}_p(pk+r) = A_1 \cup \cdots \cup A_p$. Note that for $i \leq r$ the mappings $m_i : \mathscr{A}_1(k+1) \to A_i$ defined by $m_i : x_0 \cdots x_k \mapsto 0^{i-1} x_0 0^{p-1} x_1 0^{p-1} \cdots x_{k-1} 0^{p-1} x_k 0^{r-i}$ are bijective, and the same is true of the analogous mappings $m_i : \mathscr{A}_1(k) \to A_i$ $(i > r)$. It follows that

$$|A_i| = \begin{cases} a_T(k+1) & i \leq r \\ a_T(k) & i > r. \end{cases}$$

Moreover, it is clear that all pairwise intersections of the sets A_i contain only the string 0^{pk+r}. The inclusion-exclusion principle thus gives

$$\begin{aligned}
a_{T^p}(pk+r) = |\mathscr{A}_p(pk+r)| &= |A_1| + \ldots + |A_p| + \sum_{2 \leq |J| \leq p} (-1)^{|J|-1} \binom{p}{|J|} \\
&= (p-r) a_T(k) + r a_T(k+1) + \sum_{2 \leq |J| \leq p} (-1)^{|J|-1} \binom{p}{|J|} \\
&= (p-r) a_T(k) + r a_T(k+1) - \sum_{i=2}^{p} (-1)^i \binom{p}{i} \\
&= (p-r) a_T(k) + r a_T(k+1) + (1-p) - \sum_{i=0}^{p} (-1)^i \binom{p}{i} \\
&= (p-r) a_T(k) + r a_T(k+1) + (1-p) - (1+(-1))^p \\
&= (p-r) a_T(k) + r a_T(k+1) + (1-p).
\end{aligned}$$

The case $r = 0$ follows by precisely analogous reasoning – in particular, we can use the same sets A_i as above, if we consider the symbol 0^{-1} as "backspace;" these sets then all have cardinality $a_T(k)$. This completes the proof. □

Corollary 2. *If $A_p(I;T)$ satisfies a recursion of order n, then $A_p(I;T^p)$ satisfies a recursion of order pn.*

Proof. From the last theorem, we have

$$a_{T^p}(k) = \sum_{i=0}^{p-1} a_T\left(\left\lfloor \frac{k+i}{p} \right\rfloor\right) + 1 - p \quad \text{for } k \geq p.$$

If C and K are as in the definition above, then for $k \geq p(K+1)$ we have $k \geq p$, $\lfloor \frac{k+i}{p} \rfloor \geq K$, so that

$$\begin{aligned}
a_{T^p}(k) &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\sum_{r=0}^{p-1} a_T\left(\left\lfloor \frac{\left\lfloor \frac{k+i}{p}\right\rfloor + jn + r}{p}\right\rfloor\right) + Cp + 1 - p \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\sum_{r=0}^{p-1} a_T\left(\left\lfloor \frac{\left\lfloor \frac{k+jpn+i}{p}\right\rfloor + r}{p}\right\rfloor\right) + Cp + 1 - p \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\left[a_{T^p}\left(\left\lfloor \frac{k+jpn+i}{p}\right\rfloor\right) - (1-p)\right] + Cp + 1 - p \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} a_{T^p}\left(\left\lfloor \frac{k+jpn+i}{p}\right\rfloor\right) + Cp + (1-p)(1-p^2)
\end{aligned}$$

so that a_{T^p} satisfies a recursion of order pn. The conclusion follows. □

We can now combine the above results to give the following:

Theorem 5. *Suppose p is prime, $c \in \mathbb{Z}/p$, and $n \in \mathbb{Z}^+$. Let s be the largest integer such that $p^s \mid n$. Then if $A_p(c;T)$ satisfies a recursion of order r, $A_p(c;T^n)$ satisfies a recursion of order rp^s.*

Proof. Since s is maximal, we can write $n = p^s m$, where $(p,m) = 1$. It follows that $a_{T^n}(k) = a_{T^{p^s}}(k)$ for all k, by Theorem 3, and repeated application of Corollary 2 shows that $A_p\left(c;T^{p^s}\right)$ satisfies a recursion of order rp^s. The conclusion follows. □

7 Conclusion

We have investigated recursion formulas for the line complexity sequence where the number of accessible blocks of length $2k$ is expressed in terms of the numbers of accessible blocks of several different smaller lengths. These recursions are intimately connected with the sets A_i, B_i and the maps T_{A_i}, T_{B_i} introduced above; in particular, we require these maps to be injective. The maps T_{A_i} are always injective, but the same need not be true of the maps T_{B_i}. By closely analyzing the maps T_{B_i}, we have precisely characterized the polynomials that are not suspicious, i.e. those for which the maps T_{B_i} are injective on the whole space. We have also proved that for general polynomial transition rules T, the intersection $|B_1 \cap B_2|$ is of constant size for sufficiently large k.

We have also investigated the behavior of the line complexity sequence when the transition rule is raised to different powers; by introducing a notion of the *order* of a recursion distinct from the order of the transition rule, we have seen that if an automaton modulo p with a constant initial state and a transition rule T satisfies a recursion of some order r, the automaton whose transition rule is T^n (for any n) satisfies a recursion of order rp^s, where s is the largest integer such that $p^s \mid n$.

Our results suggest the following conjecture:

Conjecture 1. *Suppose T is a polynomial transition rule that is not suspicious. Then for sufficiently large k, we have*

$$a_T(2k) = 2a_T(k) + a_T(k + \lfloor \tfrac{n}{2} \rfloor) + a_T(k + \lfloor \tfrac{n+1}{2} \rfloor) + C$$

and

$$a_T(2k+1) = a_T(k) + a_T(k+1) + a_T(k+\lfloor \tfrac{n+1}{2} \rfloor) + a_T(k+\lfloor \tfrac{n}{2} \rfloor + 1) + C,$$

where C is a constant dependent only on T.

Indeed, we have seen that the size of the intersection $B_1 \cap B_2$ stabilizes for sufficiently large k, even if T is suspicious. This raises the possibility that all intersections of A_i and B_i stabilize in size, perhaps regardless of whether T is suspicious. This is the most immediate direction of further research. Additional research directions include investigating the transformations T_{B_i} for blocks of odd length, and considering automata with coefficients taken modulo p, to see if the behaviors that arise in these situations are analogous to those we have observed in the present case.

8 Acknowledgments

I would like to thank Mr. Chiheon Kim for mentoring this project and for providing many helpful insights and suggestions. I would like to thank Prof. Pavel Etingof for suggesting this project, and Prof. Richard Stanley for suggesting the original topic. Finally, I would like to thank the MIT Math Department, the UROP+ program, and the Class of 1994 UROP fund for making this project possible.

References

[1] K. Garbe. Patterns in the coefficients of powers of polynomials over a finite field. Preprint, 2012. `http://arxiv.org/abs/1304.4635`.

[2] B. Stone. Characterization of the line complexity of cellular automata generated by polynomial transition rules. Preprint, 2014. `https://math.mit.edu/research/highschool/rsi/documents/2013Stone.pdf`.

[3] S. Janson. Resultant and discriminant of polynomials. 2010. `http://www2.math.uu.se/~svante/papers/sjN5.pdf`.