A new characterization of p-automatic sequences

Eric Rowland[1] Reem Yassawi[2]

[1]Université du Québec à Montréal

[2]Trent University

2013 April 26

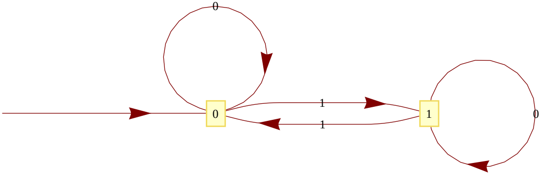
k-automatic sequences

A sequence $s(n)_{n\geq 0}$ is k-automatic if there is DFAO whose output is $s(n)$ when fed the base-k digits of n.

The Thue–Morse sequence $T(n)_{n\geq 0}$

$$0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,0\,1\,\cdots.$$

is 2-automatic:



Algebraic characterization

Let p be a prime.
Let $\mathbb{F}_q$ be a finite field of characteristic p.

Theorem (Christol–Kamae–Mendès France–Rauzy 1980)

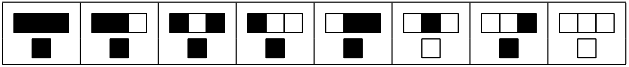
A sequence $s(n)_{n\geq 0}$ of elements in $\mathbb{F}_q$ is p-automatic if and only if the formal power series $\sum_{n\geq 0} s(n)t^n$ is algebraic over $\mathbb{F}_q(t)$.

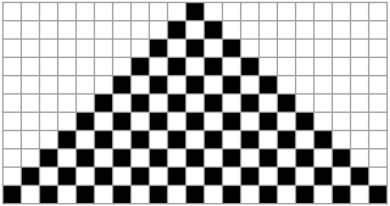
For Thue–Morse, $G(t) = \sum_{n\geq 0} T(n)t^n$ over $\mathbb{F}_2(t)$ satisfies

$$tG(t) + (1+t)G(t)^2 + (1+t^4)G(t)^4 = 0.$$

One-dimensional cellular automata

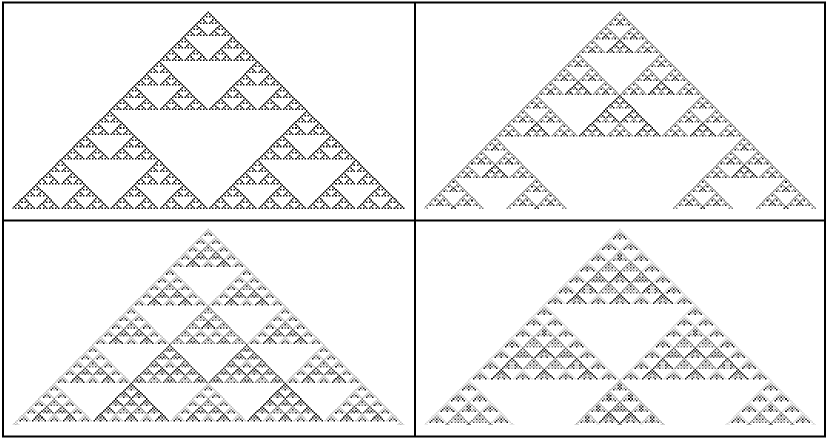
- finite alphabet Σ (for example $\{\square, \blacksquare\}$)
- function $i : \mathbb{Z} \to \Sigma$ (the initial condition)
- integer $\ell \geq 0$
- function $f : \Sigma^{\ell} \to \Sigma$ (the local update rule)





Binomial coefficients

Binomial coefficients modulo k are produced by cellular automata.



The local rule is $f(u, v, w) = u + w$ modulo k.

Linear cellular automata

A cellular automaton is linear if the local rule $f : \mathbb{F}_q^\ell \to \mathbb{F}_q$ is $\mathbb{F}_q$-linear.

For example, $f(u, v, w) = u + w$ for binomial coefficients modulo p.

Theorem (Litow–Dumas 1993)

Every column of a linear cellular automaton over $\mathbb{F}_p$ is p-automatic.

The proof uses two theorems about formal power series — Christol's theorem and a theorem of Furstenberg.

Furstenberg's theorem

The diagonal of a bivariate series $\sum_{n\geq 0}\sum_{m\geq 0} a(n,m)t^n x^m$ is

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

Theorem (Furstenberg 1967)

A formal power series $G(t)$ is algebraic over $\mathbb{F}_q(t)$ if and only if $G(t)$ is the diagonal of a bivariate rational series $F(t,x)$.

Sketch of Litow–Dumas proof

Every column of a linear cellular automaton over $\mathbb{F}_p$ is p-automatic.

Represent the nth row $\cdots\ a(n,-1)\,a(n,0)\,a(n,1)\ \cdots$ by

$$R_n(x) = \cdots + a(n,-1)x^{-1} + a(n,0)x^0 + a(n,1)x^1 + \cdots,$$

which is rational since the initial condition is eventually periodic.

Linearity of the rule means $R_{n+1}(x) = C(x)R_n(x)$ for some $C(x)$.
For binomial coefficients, $C(x) = x + \frac{1}{x}$.

Then the bivariate series $F(t,x) = \sum_{n\geq 0}\sum_{m\in\mathbb{Z}} a(n,m)t^n x^m = \sum_{n\geq 0} R_n(x)t^n = \sum_{n\geq 0}(C(x)t)^n R_0(x)$ is rational.

Column m of $F(t,x)$ is the diagonal of $x^{-m}F(tx,x)$, hence it is algebraic (Furstenberg) and hence p-automatic (Christol).

The converse

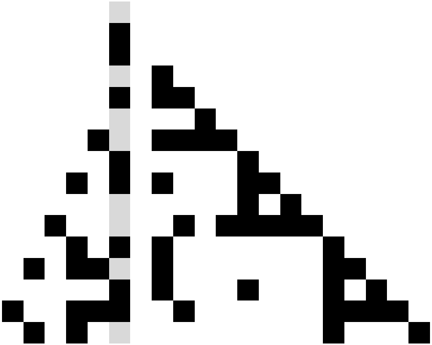
Given a p-automatic sequence, can we compute a cellular automaton?

Reverse the proof:
Christol produces a polynomial equation.
Furstenberg produces a bivariate rational series.
The denominator encodes a linear rule.

Issue 1: In general, the recurrence $C_0(x)R_n(x) = \sum_{i=1}^{d} C_i(x)R_{n-i}(x)$ will not have order 1.
To deal with this, we introduce memory into the cellular automaton.

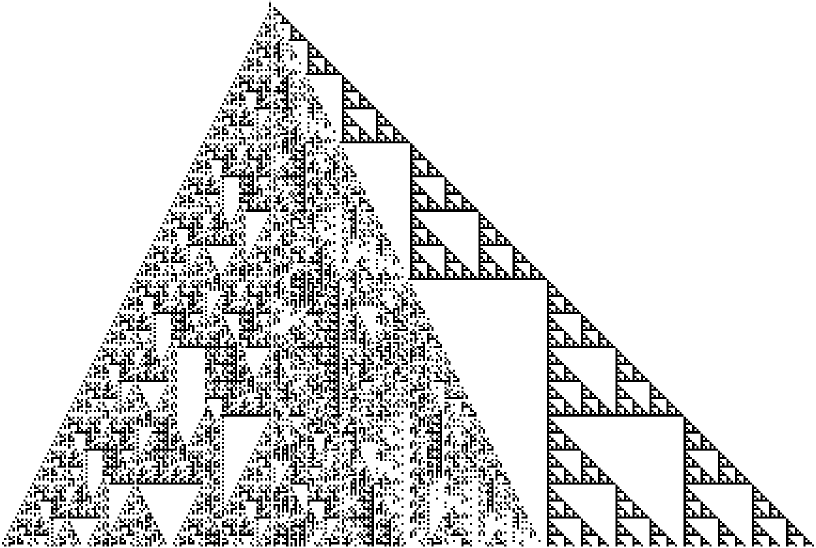
Issue 2: We need $C_0(x)$ to be a (nonzero) monomial so that each $\frac{C_i(x)}{C_0(x)}$ is a Laurent polynomial, so that the update rule is local.

Thue–Morse cellular automaton with memory 12



0
1
1
0
1
0
0
1
1
0
0
1
0
1
1
0
⋮

Thue–Morse cellular automaton with memory 12



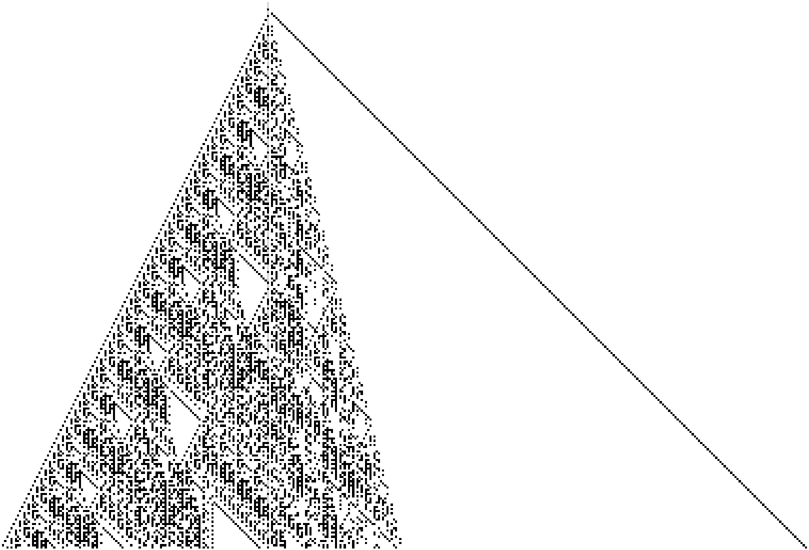
New characterization

Combined with the Litow–Dumas result, we have the following characterization of p-automatic sequences (for prime p).

Theorem

A sequence of elements in $\mathbb{F}_q$ is p-automatic if and only if it occurs as a column of a linear cellular automaton over $\mathbb{F}_q$ with memory whose initial conditions are eventually periodic in both directions.

Rudin–Shapiro cellular automaton with memory 20



Baum–Sweet cellular automaton with memory 27

The Baum–Sweet sequence 1 1 0 1 1 0 0 1 0 1 0 0 $\cdots$ is defined by

$$s(n) = \begin{cases} 0 & \text{if the binary representation of } n \\ & \quad \text{contains a block of 0s of odd length} \\ 1 & \text{if not.} \end{cases}$$