The size of the minimal automaton for an algebraic sequence

Eric Rowland
Hofstra University

Manon Stipulanti
University of Liège

Reem Yassawi
The Open University

Applications of Computer Algebra
Session on Algorithmic Combinatorics
Online, 2021–07–24

Algebraic sequences

$\mathbb{F}_q$ denotes the finite field with q elements.

Let $s(n)_{n\geq 0}$ be a sequence of elements in $\mathbb{F}_q$.

$s(n)_{n\geq 0}$ is algebraic if there exists a nonzero polynomial $P(x, y) \in \mathbb{F}_q[x, y]$ such that $P(x, \sum_{n\geq 0} s(n)x^n) = 0$.

Combinatorial motivation: Integer sequences modulo p.

Example

Catalan numbers $C(n)_{n\geq 0} = 1, 1, 2, 5, 14, 42, 132, 429, \ldots$

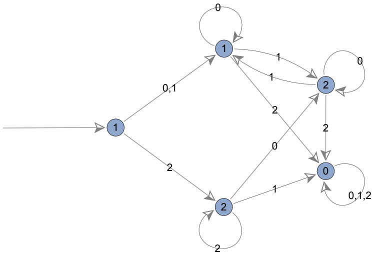
$F(x) = \sum_{n\geq 0} C(n)x^n$ satisfies $xy^2 - y + 1 = 0$ over $\mathbb{Q}$.

$F(x) = \sum_{n\geq 0}(C(n) \bmod 3)x^n$ satisfies $xy^2 + 2y + 1 = 0$ over $\mathbb{F}_3$.

Automatic sequences

A sequence $s(n)_{n \geq 0}$ is *q-automatic* there is an automaton that outputs $s(n)$ when fed the base-q digits of n.
Convention in this talk: start with the least significant digit.

This automaton computes $C(n)$ mod 3:



$C(9) = 4862 \equiv ?$ mod 3. Since $9 = 100_3$, $C(9) \equiv \boxed{2}$ mod 3.

$(C(n) \bmod 3)_{n \geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, 2, \ldots$ is 3-automatic.

Theorem (Christol 1979/1980)

A sequence $s(n)_{n\geq 0}$ of elements in $\mathbb{F}_q$ is algebraic if and only if it is q-automatic.

Two ways to represent such sequences: polynomials and automata.

How does the size of the automaton (number of states) depend on the x-degree (height) and y-degree (degree) of the polynomial?

Theorem (Bridy 2017)

Let $s(n)_{n\geq 0}$ be an algebraic sequence of elements in $\mathbb{F}_q$.
If its minimal polynomial has height h, degree d, and genus g, then the number of states in its minimal automaton is at most

$$(1 + o(1))q^{h+d+g-1},$$

where $o(1)$ tends to 0 as any of q, h, d, g gets large.

The genus satisfies $g \leq (h-1)(d-1)$; generically $g = (h-1)(d-1)$.

Corollary

The number of states is at most $(1 + o(1))q^{hd}$.

Can we get this bound without algebraic geometry? Yes.

Is the bound sharp? We suspect yes, but this is an open question.

How to construct an automaton?

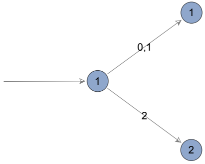
Let $r \in \{0, 1, \ldots, q-1\}$.
The Cartier operator Λ_r picks out every qth term, starting with $s(r)$:

$$\Lambda_r(s(n)_{n\geq 0}) := s(qn + r)_{n\geq 0}$$

Iteratively apply $\Lambda_0, \Lambda_1, \ldots, \Lambda_{q-1}$ to $s(n)_{n\geq 0}$.
Create one state in the automaton for each distinct sequence.

Let $s(n) = (C(n) \bmod 3)$. $\quad s(n)_{n\geq 0} = 1, 1, 2, 2, 2, 0, 0, 0, 2, \ldots$.

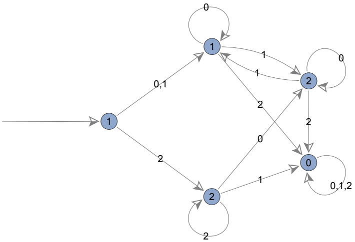
$\Lambda_0(s(n)_{n\geq 0}) = s(3n+0)_{n\geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \ldots$ new!
$\Lambda_1(s(n)_{n\geq 0}) = s(3n+1)_{n\geq 0} = 1, 2, 0, 2, 1, 0, 0, 0, 0, \ldots = \Lambda_0(s(n)_{n\geq 0})$
$\Lambda_2(s(n)_{n\geq 0}) = s(3n+2)_{n\geq 0} = 2, 0, 2, 1, 0, 0, 0, 0, 2, \ldots$ new!



Label each state with the initial term of the corresponding sequence.

$\Lambda_0(\Lambda_0(s(n)_{n\geq 0})) = 1, 2, 0, 2, 1, 0, 0, 0, 0, 2, \ldots = \Lambda_0(s(n)_{n\geq 0})$
$\Lambda_1(\Lambda_0(s(n)_{n\geq 0})) = 2, 1, 0, 1, 2, 0, 0, 0, 0, 1, \ldots$ new!
$\Lambda_2(\Lambda_0(s(n)_{n\geq 0})) = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots$ new!

$\Lambda_r(\Lambda_2(s(n)_{n\geq 0})) \quad \ldots$



A sequence is q-automatic if and only if this process terminates.

But we can't tell if sequences are equal from finitely many terms.

Use a different representation: diagonals of rational functions.

Theorem (Furstenberg 1967)

Let K be a field, and let $P(x,y) \in K[x,y]$ such that $\frac{\partial P}{\partial y}(0,0) \neq 0$. If $F(x) \in K[\![x]\!]$ satisfies $F(0) = 0$ and $P(x, F(x)) = 0$, then

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

The arguments xy arise from shearing the array of coefficients.

It will be more convenient to not shear. Then

$$F(x) = \mathcal{C}\left(\frac{y\frac{\partial P}{\partial y}(x,y)}{P(x,y)/y}\right)$$

where $\mathcal{C}$ projects a Laurent series to the column $\langle x^i y^0 : i \geq 0 \rangle$.

Example

$$\sum_{n\geq 0} (C(n) \bmod 3) x^n \text{ satisfies } xy^2 + 2y + 1 = 0 \text{ over } \mathbb{F}_3.$$

$$\sum_{n\geq 1} (C(n) \bmod 3) x^n \text{ is the } y^0 \text{ column of}$$

$$\begin{aligned}
\frac{y\frac{\partial P}{\partial y}(x,y)}{P(x,y)/y} = \frac{y(2xy+(2x+2))}{(xy^2+(2x+2)y+x)/y} = {} & 0x^0y^0 + 1x^0y^1 + 0x^0y^2 + 0x^0y^3 + 0x^0y^4 + 0x^0y^5 + \cdots \\
& + 0x^1y^{-1} + 1x^1y^0 + 0x^1y^1 + 2x^1y^2 + 0x^1y^3 + 0x^1y^4 + \cdots \\
& + 0x^2y^{-2} + 1x^2y^{-1} + 2x^2y^0 + 0x^2y^1 + 1x^2y^2 + 2x^2y^3 + \cdots \\
& + 0x^3y^{-3} + 1x^3y^{-2} + 1x^3y^{-1} + 2x^3y^0 + 0x^3y^1 + 1x^3y^2 + \cdots \\
& + 0x^4y^{-4} + 1x^4y^{-3} + 0x^4y^{-2} + 2x^4y^{-1} + 2x^4y^0 + 0x^4y^1 + \cdots \\
& + 0x^5y^{-5} + 1x^5y^{-4} + 2x^5y^{-3} + 0x^5y^{-2} + 0x^5y^{-1} + 0x^5y^0 + \cdots \\
& + \cdots .
\end{aligned}$$

We have embedded $s(n)_{n\geq 0}$ into a bivariate series $\frac{S_0}{Q}$ where $Q = P/y$.
Can we compute $\Lambda_r(s(n)_{n\geq 0})$?

Define

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

and extend linearly to power series. Define $\Lambda_{r,s}$ analogously.

The map

$$\lambda_{r,0}(S) := \Lambda_{r,0}\left(SQ^{q-1}\right)$$

on $\mathbb{F}_q[x, y]$ contains all information about $s \mapsto \Lambda_r(s)$ (and some extra):

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

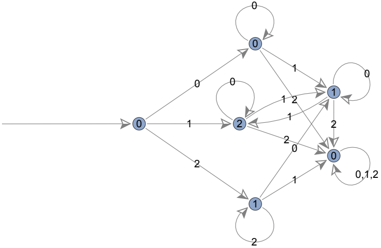
We construct an automaton by iterating $\lambda_{0,0}, \ldots, \lambda_{q-1,0}$.

$(C(n) \bmod 3)_{n \geq 1}$ is a column of $\frac{S_0}{Q} := \frac{y(2xy+2x+2)}{(xy^2+(2x+2)y+x)/y}$.

$\lambda_{0,0}(S_0) = xy + x$ new!
$\lambda_{1,0}(S_0) = 2$ new!
$\lambda_{2,0}(S_0) = y + 1$ new!

$\lambda_{0,0}(xy + x) = xy + x = \lambda_{0,0}(S_0)$ ...

If two polynomials are equal, the corresponding sequences are equal.



The automaton may not be minimal.

Let $V := \langle x^i y^j : 0 \le i \le h \text{ and } 0 \le j \le d-1 \rangle$. $\dim V = (h+1)d$

Proposition

For each $r \in \{0, 1, \dots, q-1\}$, we have $\lambda_{r,0}(S_0) \in V$.
For each $r \in \{1, \dots, q-1\}$,

$$\lambda_{r,0}(V) \subseteq \left\langle x^i y^j : 0 \le i \le h-1 \text{ and } 0 \le j \le d-1 \right\rangle$$

which has dimension hd.

Corollary:
The constructed automaton has at most $q^{hd} + |\mathrm{orb}_{\lambda_{0,0}}(S_0)|$ states.

It remains to bound $|\mathrm{orb}_{\lambda_{0,0}}(S_0)|$.

Certain orders of the basis for V show that $\lambda_{0,0}$ is highly structured.

Example

Let $q = 3$, $h = 2$, $d = 4$, and

$$P = (x^2 + x + 2)y^4 + xy^3 + (2x + 1)y^2 + (x^2 + 1)y + 2x^2 + x.$$

Basis:

$$\left(x^1y^0, x^1y^1, x^1y^2, \quad x^0y^1, x^0y^2, \quad x^0y^0, \quad x^1y^3, \quad x^0y^3, \quad x^2y^0, x^2y^1, x^2y^2, \quad x^2y^3\right).$$

Matrix for $\lambda_{0,0}$:

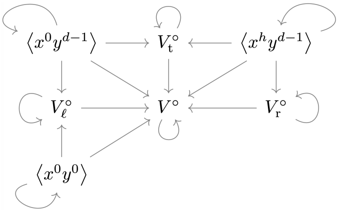
$$\begin{bmatrix}
1 & 1 & 1 & 2 & 1 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
1 & 2 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 2 \\
2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 1 & 1 & 1 \\
 & & & 1 & 2 & 1 & & 1 & & & & \\
 & & & 0 & 1 & 1 & & 1 & & & & \\
 & & & & & 1 & & & & & & \\
 & & & & & & 2 & 2 & & & & 1 \\
 & & & & & & & 1 & & & & \\
 & & & & & & & & 1 & 1 & 1 & 0 \\
 & & & & & & & & 2 & 1 & 0 & 1 \\
 & & & & & & & & 1 & 0 & 0 & 2 \\
 & & & & & & & & & & & 1
\end{bmatrix}$$

Basis of V:

x^0y^{d-1}	x^1y^{d-1}	$\cdots$	$x^{h-1}y^{d-1}$	x^hy^{d-1}
x^0y^{d-2}	x^1y^{d-2}	$\cdots$	$x^{h-1}y^{d-2}$	x^hy^{d-2}
$\vdots$	$\vdots$	$\iddots$	$\vdots$	$\vdots$
x^0y^1	x^1y^1	$\cdots$	$x^{h-1}y^1$	x^hy^1
x^0y^0	x^1y^0	$\cdots$	$x^{h-1}y^0$	x^hy^0

Theorem

Under applications of $\lambda_{0,0}$ on V, information flows as follows.



The left, right, and top subspaces are affected only by themselves.
Since $|V^\circ| = q^{(h-1)(d-1)}$, we show the borders contribute $\leq q^{h+d-1}$.

The left, right, and top subspaces are essentially univariate.

Fix $R \in \mathbb{F}_q[z]$. How big are orbits under $\lambda_0(S) := \Lambda_0\big(SR^{q-1}\big)$?
This is "just" a linear transformation.

Example

Let $q = 3$ and $R = (z^2 + 1)(z^3 + z^2 + 2) \in \mathbb{F}_3[z]$.
Compute $\mathrm{orb}_{\lambda_0}(S)$ from each $S \in \mathbb{F}_3[z]$ with $\deg S \leq \deg R$.
Period lengths that occur: $\{1, 2, 3, 6\}$

Example

Let $q = 3$ and $R = (z^2 + 1)(z^4 + z + 2) \in \mathbb{F}_3[z]$.
Period lengths: $\{1, 2, 4\}$

Consider all polynomials R with fixed degree.
Surprising fact: The maximal period length doesn't depend on q.

Theorem

Let $R \in \mathbb{F}_q[z]$ such that $R \neq 0$, $z \nmid R$, and R is square-free. Let $cR_1 \cdots R_m$ be its factorization into irreducibles, and let

$$\ell = \operatorname{lcm}(\deg R_1, \dots, \deg R_m).$$

Then $\lambda_0^\ell(S) = S$ for all $S \in \mathbb{F}_q[z]$ with $\deg S \leq \deg R$.

The upper bound is achieved when ℓ is maximized, subject to $\deg R_1 + \cdots + \deg R_m = \deg R$.

The Landau function $L(n)$ is the maximum value of $\operatorname{lcm}(n_1, \dots, n_m)$ over all integer partitions $(n_1, \dots, n_m)$ of n. Also arises in Bridy's proof.

Corollary

The number of states is at most

$$q^{hd} + q^{(h-1)(d-1)} L(h) L(d)^2 + \left\lceil \log_q \max(h, d, q) \right\rceil.$$

Asymptotically…

Landau (1903): $\log L(n) \sim \sqrt{n \log n}$

Massias–Nicolas–Robin (1988): $L(n) \le e^{(1+o(1))\sqrt{n \log n}}$

Corollary

The number of states is at most $(1 + o(1))q^{hd}$.

Example

The factor $1 + o(1)$ cannot be removed. Let $q = 2$ and

$$P = (x^3 + x^2 + 1)y^3 + (x^3 + 1)y^2 + (x^3 + x^2 + x + 1)y + x^3 + x^2$$

with $h = 3$ and $d = 3$. The number of states is $532 > 512 = q^{hd}$.

References

- Andrew Bridy, Automatic sequences and curves over finite fields, *Algebra & Number Theory* **11** (2017) 685–712.
- Gilles Christol, Ensembles presque periodiques *k*-reconnaissables, *Theoretical Computer Science* **9** (1979) 141–145.
- Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy, Suites algébriques, automates et substitutions, *Bulletin de la Société Mathématique de France* **108** (1980) 401–419.
- Harry Furstenberg, Algebraic functions over finite fields, *Journal of Algebra* **7** (1967) 271–277.
- Edmund Landau, Über die Maximalordung der Permutation gegbenen Grades, *Archiv der Mathematik und Physik* Series 3, **5** (1903) 92–103.
- J.-P. Massias, J.-L. Nicolas, and G. Robin, Évaluation asymptotique de l'ordre maximum d'un élément du groupe symétrique, *Acta Arithmetica* **50** (1988) 221–242.