A quantitative version of Christol's theorem

Reem Yassawi

Université Claude Bernard Lyon 1, France

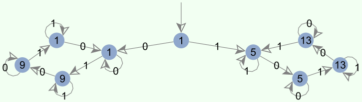
June 29, 2019

Automatic sequences

Definition

A sequence $(a_n)_{n\geq 0}$ of elements in $\mathcal{A}$ is k-*automatic* if there is a DFAO $(\mathcal{S}, \Sigma_k, \delta, s_0, \mathcal{A}, \omega)$ such that $a_n = \omega(\delta(s_0, n_\ell \cdots n_1 n_0))$ for all $n \geq 0$, where $n_\ell \cdots n_1 n_0$ is the standard base-k representation of n, fed in reverse reading.

Example (Apéry numbers mod 16)



The 2*-automatic sequence produced by this automaton is*

$$(a_n)_{n\geq 0} = 1, 5, 9, 5, 9, 13\ldots$$

Theorem (Christol 1979) *Let $S \subset \mathbb{N}$ and let $a_n = 1$ if $n \in S$, $a_n = 0$ otherwise. Then $(a_n)_{n\geq 0}$ is p-automatic if and only if $\sum_{n\in S} x^n$ is algebraic over $\mathbb{F}_p(x)$.*

Theorem (Christol–Kamae–Mendès France–Rauzy 1980) *Let $(a_n)_{n\geq 0}$ be a sequence in $\mathbb{F}_q$. Then $(a_n)_{n\geq 0}$ is p-automatic if and only if $\sum_{n\geq 0} a_n x^n$ is algebraic over $\mathbb{F}_q(x)$.*

Definition

Let $\mathbf{a} = (a_n)_{n\geq 0}$ be a p-automatic sequence. The reverse (direct) reading complexity of $\mathbf{a}$, denoted $\mathrm{comp}_q(\mathbf{a})$ ($\overrightarrow{\mathrm{comp}}_q(\mathbf{a})$), is the size of the minimal automaton generating $\mathbf{a} = (a_n)_{n\geq 0}$ in reverse (direct) reading.

Question: If $A(x, y)$ has height h and degree d, what is an upper limit for $\mathrm{comp}_q(\mathbf{a})$ or $\overrightarrow{\mathrm{comp}}_q(\mathbf{a})$, in terms of d and h?

Theorem (Christol, quantitative) *If* $f(x) = \sum_{n\geq 0} a_n x^n$ *is annihilated by* $A(x, y)$ *of height* h *and degree* d*, then* $\mathrm{comp}_q(\mathbf{a})$

1. *can be made explicit*
   (Harase, 88, 89)
2. *is at most* $q^{qd(h(2d^2-2d+1)+C(q))}$.
   (Fresnel, Koskas, de Mathan, 2000.)
3. *is at most* $q^{d^4h^2q^{5d}}$,
   is at most q^A*, where* $A = A(h, d)$.
   (Adamczewski, Bell, 2012, 2013.)
4. *is at most* $q^{hd}(1 + o(1))$ *for large values of* q*,* d *or* h.
   (Bridy, 2016.)
5. *is at most* $q^{(h+1)d+1}(1 + o(1))$ *for large values of* q*,* d*, or* h.
   (Adamczewski, Y, 2019.)

The tools: The Cartier operators

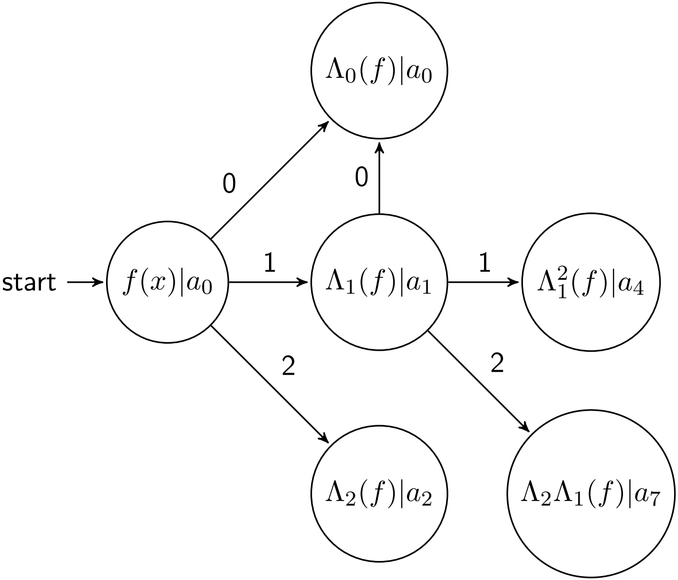
Let $\ell \in \{0, 1, \ldots, q-1\}$. The Cartier operator $\Lambda_\ell : \mathbb{F}_q[[x]] \to \mathbb{F}_q[[x]]$ is the map defined by

$$\Lambda_\ell \left(\sum_{n \geq 0} a_n x^n \right) := \sum_{n \geq 0} a_{qn+\ell} x^n.$$

Let Ω_1 denote the monoid generated by these operators under composition.
We call $\Omega_1(f)$ the q-kernel of $\mathbf{a}$.

Theorem (Eilenberg) *The sequence $\mathbf{a} = (a_n)_{n \geq 0}$ is q-automatic if and only if it has a finite q-kernel. Moreover, $|\Omega_1(f)| = \mathrm{comp}_q(\mathbf{a})$.*

Labelling a minimal automaton for $\mathbf{a}$ with $\Omega_1(f)$



Proof of "algebraic implies automatic" in CKMR, 1980

Input: $A(x,y) \in \mathbb{F}_q[x,y]$, degree d, height h, with $A(x, f(x)) = 0$.
Strategy: Find an $\mathbb{F}_q$-vector space V of finite dimension which contains $f(x)$, such that $\Omega_1(V) \subset V$.
Tool: Use an Ore polynomial to define V:

$$A_0(x)f(x) = \sum_{i=1}^{d} A_i(x)(f(x))^{q^i}.$$

Consider

$$V = \left\{ \sum_{i=1}^{d} C_i(x) f^{q^i} : \deg(C_i(x)) \leq N \right\},$$

then $\Omega_1(V) \subset V$, and $\dim_{\mathbb{F}_q}(V) \leq dN$, so $\mathrm{comp}_q(\mathbf{a}) \leq q^{dN}$.
Problem: N is exponential in q.

Speyer's proof of Christol's theorem

Input: $A(x, y) \in \mathbb{F}_q[x, y]$, degree d, height h, with $A(x, f(x)) = 0$.
Strategy: Find an $\mathbb{F}_q$-vector space V of finite dimension which "contains" $f(x)$, such that $\tilde{\Omega}_1(V) \subset V$.
Tool: Use the Riemann-Roch theorem to find vector spaces V which are $\tilde{\Omega}_1$ invariant.
Consider the variety $\mathcal{V}_A = \{(x, y) \in \mathbb{P}_q \times \mathbb{P}_q : A(x, y) = 0\}$, where we assume that the curve defined by $A(x, y) = 0$ is projective and nonsingular.
Let K_A be $\mathcal{V}_A$'s function field, and let

$\mathcal{K}_A = \{g(x)dx : g(x) \in K_A, x$ is a separating variable, i.e. $x \notin K_A^p\}$.

Theorem (Riemann-Roch) *Given an effective divisor D,*

$$V_D := \{f(x)dx \in \mathcal{K}_A : \nu_P(f(x)dx) \geq -D_P\}$$

is a vector space of dimension $\deg(D) + g - 1$ *over* $\mathbb{F}_p$.

Bridy's quantification of Speyer's proof

The Cartier operator $\tilde{\Lambda}_{p-1} : \mathcal{K}_A \to \mathcal{K}_A$ is defined by

$$\tilde{\Lambda}_{p-1}\left(\sum_n a_n x^n dx\right) := \sum_{n=0}^{\infty} a_{np+p-1}^{1/p} x^n dx$$

and it captures where $f dx$ will have residues.

Theorem (Bridy, 2016) *Let D be the divisor generated by $f(x)dx$. Then*

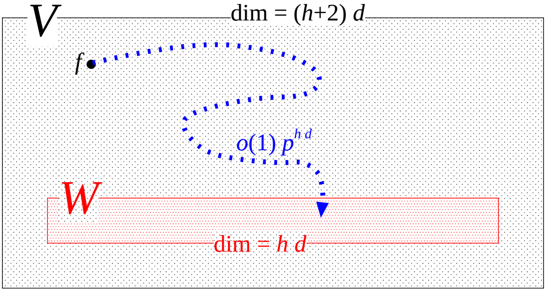
$$\tilde{\Omega}_1(V_D) \subset V_D,$$

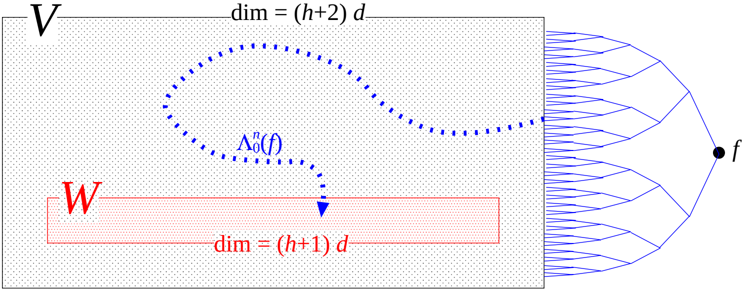
and V_D has $\mathbb{F}_q$-dimension $h + 3d + g - 1 \leq hd + 2d = (h+2)d$.

Theorem (Bridy, 2016) *There exist nested vector spaces $W \subset V$, of $\mathbb{F}_q$-dimension hd and $(h+2)d$, such that $\Omega_1(f) \subset V$ and $|\Omega_1(f) \backslash W| = o(1)q^{hd}$. Thus*

$$|\mathrm{comp}_q(\mathbf{a})| \leq q^{hd}(1 + o(1)).$$

Bridy's and our proof in pictures





Christol's first proof of his theorem (1979)

Theorem (Furstenberg, 1967) *Let κ be a field and let $A(x,y) \in \kappa[x,y]$. Let $f(x) \in x\kappa[[x]]$ be a root of $A(x,y)$. If $\frac{\partial A}{\partial y}(0,0) \neq 0$ then*

$$f(x) = \Delta\left(\frac{y\frac{\partial A}{\partial y}(xy,y)}{y^{-1}A(xy,y)}\right).$$

$$\begin{aligned}
\Lambda_\ell(f) &= \Lambda_\ell\left(\Delta\left(\frac{y\frac{\partial A}{\partial y}(xy,y)}{y^{-1}A(xy,y)}\right)\right) = \Delta\left(\Lambda_{\ell,\ell}\left(\frac{y\frac{\partial A}{\partial y}(xy,y)}{y^{-1}A(xy,y)}\right)\right)\\
&= \Delta\left(\frac{\Lambda_{\ell,\ell}\left(y\frac{\partial A}{\partial y}(xy,y)y^{1-q}A(xy,y)^{q-1}\right)}{y^{-1}A(xy,y)}\right)
\end{aligned}$$

Finishing Christol's proof in the nonsingular case

$$\Lambda_\ell(f) = \Delta\left(\frac{\Lambda_{\ell,\ell}\left(y\frac{\partial A}{\partial y}(xy,y)y^{1-q}A(xy,y)^{q-1}\right)}{y^{-1}A(xy,y)}\right),$$

hence if $A(x,y)$ is nonsingular at the origin and $A(0,0)=0$,

$$V := \operatorname{span}_{\mathbb{F}_q}\left\{\left(\frac{(xy)^i y^j}{y^{-1}A(xy,y)}\right) : 0 \le i \le h, 0 \le j \le d\right\}$$

is $\Lambda_{\ell,\ell}$-invariant and $\Omega_1(f) \subset \Delta(V)$. So $\operatorname{comp}_q(\mathbf{a}) \le q^{(h+1)(d+1)}$.
With a tiny bit more care we have:

Theorem (Adamczewski-Y) *If $f(x) = \sum_{n\ge 0} a_n x^n$ is annihilated by $P(x,y)$, with $\frac{\partial A}{\partial y}(0,0) \ne 0$ and $A(0,0)=0$, then $\operatorname{comp}_q(\mathbf{a}) \le 1 + q^{(h+1)d}$.*

Finishing Christol's proof in the singular case

If $A(x, y)$ is singular at the origin, let r be the order at 0 of the resultant of $A(x, y)$ and $\frac{\partial A}{\partial y}(x, y)$. We can explicitly define polynomials $M(x, y)$, such that after a little $o(1)q^{hd}$ trip, the Cartier operators applied to f land in $\Delta(V)$, where

$$V := \mathrm{span}_{\mathbb{F}_q} \left\{ \frac{(xy)^i M(xy, y)^j}{y^{-1}A(xy, y)} : r - 1 \leq i \leq h + r, 0 \leq j \leq d - 1 \right\}.$$

Theorem (Adamczewski-Y) *Let $f(x) = \sum_{n \geq 0} a_n x^n \in \mathbb{F}_q[[x]]$ be an algebraic power series of degree d and height h. Then*

$$\mathrm{comp}_q(\mathbf{a}) \leq (1 + o(1))q^{(h+1)d+1},$$

where the $o(1)$ term tends to 0 for large values of any of q, h, or d.

Implications for the size of direct reading automata

Let $f(x) = \sum a_n x^n \in \mathbb{F}_q[[x]]$ be algebraic over $\mathbb{F}_q(x)$, annihilated by $A(x, y)$ of degree d and height h.

Theorem (Bridy, 2016) *The forward and reverse reading complexity of $\mathbf{a}$ are at most $q^{(h+1)d}$.*

Theorem (Adamczewski,Y, 2019) *Let r be the order at 0 of the resultant of $A(x, y)$ and $\frac{\partial A}{\partial y}(x, y)$. Then the forward and reverse reading complexity of $\mathbf{a}$ are at most $q^{(h+1)d+1+r}$.*
In particular, $\overrightarrow{\mathrm{comp}}_q(\mathbf{a}) \leq q^{(3h+1)d-h+1}$.

The interpretation of the genus g

"The genus g of y will be the genus of the normalization of the projective closure of the affine plane curve defined by the minimal polynomial of y."

Definition (via Riemann-Roch)

The genus is $g := \dim(V_D) - \deg(D) + 1$ for any effective divisor D.

Theorem (Bridy, 2016) *Let $f(x) = \sum a_n x^n \in \mathbb{F}_q[[x]]$ be algebraic over $\mathbb{F}_p(x)$, annihilated by $A(x,y)$ of degree d, height h and genus g The forward and reverse reading complexity of (a_n) is at most $q^{h+2d+g-1}$.*

Theorem (Beelen 2009) *Let $\mathcal{P}$ be the Newton polygon of $A(x,y)$, and let g_A be the number of integral points in the interior of $\mathcal{P}$. If $A(x,y)$ is irreducible over $\mathbb{F}_q$, then $g \leq g_A$.*

We can formulate similar bounds to Bridy's using g_A instead of g.

Tightness of bounds?

Theorem (Bridy) *If $d = 1$, then for every prime power q and every positive integer $h \geq 1$ there exists a polynomial $A(x, y)$ whose root has a q-kernel with at least q^h elements.*

Open question

If $d \geq 2$, are these bounds tight?

Open question

Can one easily bound the orbit of $\{\Lambda_0^n(f) : n \geq 0\}$?

The strengths and limits of Furstenberg's method

Strengths:

- Extension to functions of several variables over any field,
- Extension to bounding (automaton) complexity of integer sequences $\mathbf{a} \mod p^\alpha$, for almost all p and any diagonal $\mathbf{a}$.

Theorem (Denef-Lipshitz, 1987) *If* $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Z}_p[[x]]$ *is algebraic over* $\mathbb{Z}_p(x)$*, then* $\mathbf{a} \bmod p^\alpha$ *is* p*-automatic for any* $\alpha \in \mathbb{N}$.

Limits:

Example *Let* $z = \sum_{n\geq 0} T_n x^n$ *be the generating function of the sequence of central trinomial coefficients. It satisfies*

$$P(x, z) = (x + 1)(3x - 1)z^2 + 1 = 0.$$

For every $\alpha \in \mathbb{N}$ $(T_n \mod 2^\alpha)_{n\geq 0}$ *is 2-automatic. However* $P(x, y) \mod 2$ *is not irreducible, so no separation of roots is possible and we cannot apply Furstenberg's theorem to compute* $(T_n \bmod 2^\alpha)_{n\geq 0}$*. Are there any efficient techniques to do this?*