Algebraic power series and their automatic complexity

Eric Rowland
Hofstra University

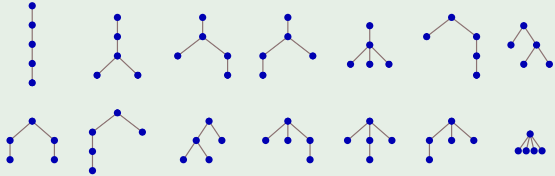
Joint work with Manon Stipulanti and Reem Yassawi

One World Seminar on Combinatorics on Words
2024–02–06

What do combinatorial sequences look like modulo p^α?

Example

Catalan numbers count plane trees with n edges:



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

Modulo 2: $1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \ldots$

$C(n)$ is odd if and only if $n + 1$ is a power of 2.
(follows from Kummer 1852)

Modulo 4: $1, 1, 2, 1, 2, 2, 0, 1, 2, 2, 0, 2, 0, 0, 0, 1, \ldots$

Theorem (Eu–Liu–Yeh 2008)

For all $n \geq 0$,

$$C(n) \bmod 4 = \begin{cases} 1 & \text{if } n+1 = 2^a \text{ for some } a \geq 0 \\ 2 & \text{if } n+1 = 2^b + 2^a \text{ for some } b > a \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $C(n) \not\equiv 3 \mod 4$.

Modulo 8: $1, 1, 2, 5, 6, 2, 4, 5, 6, 6, 4, 2, 4, 4, 0, 5, \ldots$

Theorem 4.2. *Let C_n be the nth Catalan number. First of all, $C_n \not\equiv_8 3$ and $C_n \not\equiv_8 7$ for any n. As for other congruences, we have*

$$C_n \equiv_8 \begin{cases} 1 & \text{if } n = 0 \text{ or } 1; \\ 2 & \text{if } n = 2^a + 2^{a+1} - 1 \text{ for some } a \geq 0; \\ 4 & \text{if } n = 2^a + 2^b + 2^c - 1 \text{ for some } c > b > a \geq 0; \\ 5 & \text{if } n = 2^a - 1 \text{ for some } a \geq 2; \\ 6 & \text{if } n = 2^a + 2^b - 1 \text{ for some } b - 2 \geq a \geq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Liu and Yeh (2010) determined $C(n)$ mod 16:

Theorem 5.5. *Let c_n be the n-th Catalan number. First of all, $c_n \not\equiv_{16} 3, 7, 9, 11, 15$ for any n. As for the other congruences, we have*

$$c_n \equiv_{16} \begin{cases} \left.\begin{array}{c} 1 \\ 5 \\ 13 \end{array}\right\} & \text{if} \quad d(\alpha) = 0 \ \text{and} \quad \begin{cases} \beta \le 1, \\ \beta = 2, \\ \beta \ge 3, \end{cases} \\ \left.\begin{array}{c} 2 \\ 10 \end{array}\right\} & \text{if} \quad d(\alpha) = 1,\ \alpha = 1 \ \text{and} \quad \begin{cases} \beta = 0 \ \text{or} \ \beta \ge 2, \\ \beta = 1, \end{cases} \\ \left.\begin{array}{c} 6 \\ 14 \end{array}\right\} & \text{if} \quad d(\alpha) = 1,\ \alpha \ge 2 \ \text{and} \quad \begin{cases} (\alpha = 2, \beta \ge 2) \ \text{or} \ (\alpha \ge 3, \beta \le 1), \\ (\alpha = 2, \beta \le 1) \ \text{or} \ (\alpha \ge 3, \beta \ge 2), \end{cases} \\ \left.\begin{array}{c} 4 \\ 12 \end{array}\right\} & \text{if} \quad d(\alpha) = 2 \ \text{and} \quad \begin{cases} zr(\alpha) \equiv_2 0, \\ zr(\alpha) = 1, \end{cases} \\ \quad 8 & \text{if} \quad d(\alpha) = 3, \\ \quad 0 & \text{if} \quad d(\alpha) \ge 4. \end{cases}$$

where $\alpha = (CF_2(n+1) - 1)/2$ and $\beta = \omega_2(n+1)$ (or $\beta = \min\{i \mid n_i = 0\}$).

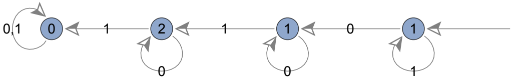
They also determined $C(n)$ mod 64.

Better framework: automatic sequences.

Automatic sequences

$s(n)_{n \geq 0}$ is p-automatic if there is an automaton that outputs $s(n)$ when fed the base-p digits of n (least significant digit first).

$C(n) \bmod 4$:

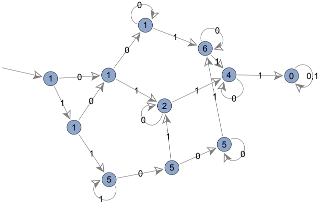


$C(9) \equiv ? \mod 4$.

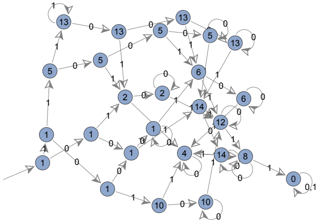
Since $9 = 1001_2$, $C(9) \equiv \boxed{2} \mod 4$.

$(C(n) \bmod 4)_{n \geq 0} = 1, 1, 2, 1, 2, 2, 0, 1, 2, 2, \dots$ is 2-automatic.

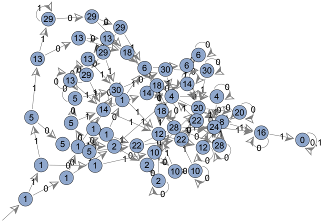
mod 8:



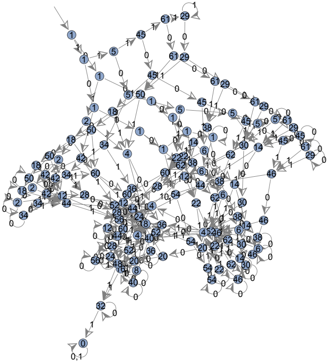
mod 16:



mod 32:



mod 64:



$(C(n) \bmod p^\alpha)_{n\geq 0}$ is p-automatic for each $\alpha \geq 1$.

The sequence of Catalan numbers is algebraic:

$$F = \sum_{n \geq 1} C(n) x^n \quad \text{satisfies} \quad x\,(F+1)^2 - F = 0.$$

Omit $C(0) = 1 \neq 0$.

Convert to the diagonal of a rational series (Furstenberg 1967):
$P = x(y+1)^2 - y$, so

$$F = \operatorname{diag}\left(\frac{y \frac{\partial P}{\partial y}(xy, y)}{P(xy, y)/y}\right) = \operatorname{diag}\left(\frac{y - 2xy^2 - 2xy^3}{1 - x - 2xy - xy^2}\right).$$

Theorem (Denef–Lipshitz 1987)

Let $\alpha \geq 1$. Let $S(\mathbf{x}), Q(\mathbf{x}) \in \mathbb{Z}_p[\mathbf{x}]$ such that $Q(0, \dots, 0) \not\equiv 0 \mod p$. Then the coefficient sequence of $\left(\operatorname{diag} \frac{S(\mathbf{x})}{Q(\mathbf{x})}\right) \mod p^\alpha$ is p-automatic.

$\mathbb{Z}_p$ is the set of p-adic integers.

Automaton size

How big is the (unminimized) automaton for $(C(n) \bmod 2^\alpha)_{n \geq 1}$?

α	1	2	3	4	5	6	7	8	9
size	4	6	15	37	83	194	445	1034	2403
$1.4 \times 2.3^\alpha$	3.2	7.4	17.0	39.2	90.1	207.3	476.7	1096.4	2521.6

height $h = \deg_x P$
degree $d = \deg_y P$
Upper bound from the construction: $p^{p^{2(\alpha-1)}\alpha h d}$

Example

$C(n) \bmod 2^9$: $P = x(y+1)^2 - y$ $h = 1$ $d = 2$
size $\leq 2^{18 \cdot 2^{16}} = 2^{1179648}$

Why is the bound so large?

Simpler setting: finite fields.

Finite fields

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 representations: polynomials and automata.

Theorem (Bridy 2017)

If the minimal polynomial P has height h and degree d, then the minimal automaton has size at most

$$(1 + o(1))q^{hd}$$

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

Is the bound sharp? We suspect yes.

Polynomials in $\mathbb{F}_q[x, y]$ with maximum unminimized automaton size:

$q = 2$:

h	d	P	aut. size	q^{hd}	bound
1	2	$xy^2 + (x+1)y + x$	7	4	9
2	2	$x^2y^2 + (x^2+x+1)y + x^2$	14	16	25
3	2	$(x^3+x^2+1)y^2 + (x^3+1)y + x$	68	64	94
4	2	$(x^4+x+1)y^2 + (x^4+x^2+x+1)y + x$	252	256	311
5	2	$(x^5+x^3+1)y^2 + (x^5+x+1)y + x$	1052	1024	1192
6	2	$(x^6+x^5+1)y^2 + (x^6+x^2+x+1)y + x$	4062	4096	4424
7	2	$(x^7+x+1)y^2 + (x^7+x^4+x^3+x+1)y + x$	16424	16384	17288
1	3	$xy^3 + y^2 + (x+1)y + x$	11	8	18
2	3	$(x^2+x+1)y^3 + y^2 + (x^2+1)y + x^2 + x$	61	64	93
3	3	$(x^3+x+1)y^3 + y^2 + (x^3+x^2+x+1)y + x^3 + x^2$	533	512	614
4	3	$(x^4+x+1)y^3 + y^2 + (x^4+1)y + x^4 + x^3 + x$	4213	4096	4871
1	4	$(x+1)y^4 + y^2 + (x+1)y + x$	20	16	33
2	4	$(x^2+x+1)y^4 + y^3 + (x^2+x+1)y + x^2 + x$	216	256	358
3	4	$(x^3+x+1)y^4 + y^3 + (x^3+1)y + x^2 + x$	3956	4096	4870
1	5	$(x+1)y^5 + (x+1)y^2 + y + x$	37	32	67
2	5	$(x^2+x+1)y^5 + y^4 + y^3 + x^2y^2 + y + x^2 + x$	889	1024	1510
3	5	$(x^3+x^2+1)y^5 + y^4 + x^3y^2 + (x+1)y + x^3 + x^2 + x$	43913	32768	48134

$q = 3$:

h	d	P	aut. size	q^{hd}	bound
1	2	$(x+1)y^2 + y + x$	9	9	14
2	2	$(x^2+x+2)y^2 + y + x^2$	79	81	91
3	2	$(x^3+x^2+2x+1)y^2 + y + x^3 + x$	727	729	788
4	2	$(x^4+x^3+2)y^2 + y + x^4 + x$	6533	6561	6729

Can we get Bridy's bound without algebraic geometry? Yes.

Theorem (Rowland–Stipulanti–Yassawi 2023)

The minimal automaton has size at most

$$q^{hd} + q^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \lfloor \log_q h \rfloor + \lceil \log_q \max(h, d-1) \rceil + 3.$$

$P \in \mathbb{F}_q[x,y], \quad h = \deg_x P, \quad d = \deg_y P$

Corollary (Bridy)

The minimal automaton has size at most $(1 + o(1))q^{hd}$.

Step 1

size $\leq q^{(h+1)d} + 1$.

$F = \operatorname{diag}\left(\frac{y\frac{\partial P}{\partial y}(xy,y)}{P(xy,y)/y}\right) = [y^0]\left(\frac{y\frac{\partial P}{\partial y}}{P/y}\right)$ sheared Let $S_0 = y\frac{\partial P}{\partial y}$, $Q = P/y$.

One Cartier operator for each digit $0, 1, \ldots, q-1$. Ex. If $q = 3$, then

$$\Lambda_1\left(a_0 + a_1 x + a_2 x^2 + \cdots\right) = a_1 + a_4 x + a_7 x^2 + \cdots .$$

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

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

Proposition

If $S \in \mathbb{F}_q[x,y]$ with $\deg_x S \leq h$ and $\deg_y S \leq d$, then

- $\deg_x \lambda_{0,0}(S) \leq h$ *and* $\deg_x \lambda_{r,0}(S) \leq h-1$ *for* $r \in \{1, \ldots, q-1\}$.
- $\deg_y \lambda_{r,0}(S) \leq d-1$ *for* $r \in \{0, 1, \ldots, q-1\}$.

Goal:

$$\boxed{q^{hd} + q^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \lfloor \log_q h \rfloor + \lceil \log_q \max(h, d-1) \rceil + 3}$$

Step 2

size $\leq q^{hd} + |\mathrm{orb}_{\Lambda_0}(F)|$.

$\mathbb{F}_q$-vector space of polynomials with size q^{hd}:

$$W := \left\langle x^i y^j : 0 \leq i \leq h-1 \text{ and } 0 \leq j \leq d-1 \right\rangle$$

Proposition

$\lambda_{r,0}(W) \subseteq W$ *for each* $r \in \{0, 1, \ldots, q-1\}$.

Therefore every state outside $\mathrm{orb}_{\Lambda_0}(F)$ is in W.

Goal:

$$\boxed{q^{hd} + q^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \lfloor \log_q h \rfloor + \lceil \log_q \max(h, d-1) \rceil + 3}$$

Step 3

$$|\mathrm{orb}_{\Lambda_0}(F)| \leq q^{(h-1)(d-1)}\mathcal{L}(h,d,d) + \lfloor \log_q h \rfloor + \lceil \log_q \max(h, d-1) \rceil + 3.$$

$\mathcal{L}(l,m,n)$ is related to the Landau function $g(n)$:

$$g(5) = \max(\mathrm{lcm}(5), \mathrm{lcm}(4,1), \mathrm{lcm}(3,2), \mathrm{lcm}(3,1,1), \mathrm{lcm}(2,2,1), \mathrm{lcm}(2,1,1,1), \mathrm{lcm}(1,1,1,1,1)) = 6$$

We'll have 3 univariate polynomials R, with degrees $\leq h, d, d$.

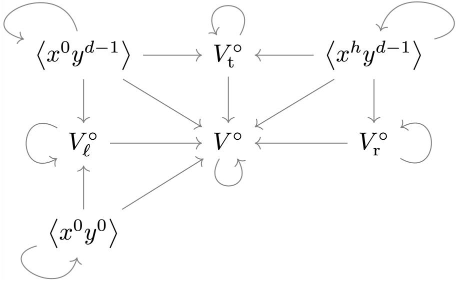
Factor each $R = R_1^{e_1} \cdots R_k^{e_k}$. $\longrightarrow$ period length $\mathrm{lcm}(\deg R_1, \dots, \deg R_k)$ and transient length $\log_q \max(e_1, \dots, e_k)$

$$\mathcal{L}(h,d,d) = \max_{\substack{1 \leq i \leq h \\ 1 \leq j \leq d \\ 1 \leq k \leq d}} \max_{\substack{\sigma_1 \in \mathrm{partitions}(i) \\ \sigma_2 \in \mathrm{partitions}(j) \\ \sigma_3 \in \mathrm{partitions}(k)}} \mathrm{lcm}(\mathrm{lcm}(\sigma_1), \mathrm{lcm}(\sigma_2), \mathrm{lcm}(\sigma_3))$$

Basis of $V \supseteq W$:

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

Information flow under $\lambda_{0,0}$:



$\lambda_0(S) = \Lambda_0(SR^{q-1})$ emulates $\lambda_{0,0}$ on each border.

Write $P = \sum_{i=0}^{h} x^i A_i(y) = \sum_{j=0}^{d} B_j(x) y^j$.
The 3 polynomials R are B_d, A_0, A_h, which have degrees $\leq h, d, d$.

How do we get period length $\ell = \operatorname{lcm}(\deg R_1, \ldots, \deg R_k)$?

Theorem

Let $R \in \mathbb{F}_q[z]$ be a square-free polynomial with $R(0) \neq 0$ and $\deg R \geq 1$. Factor $R = cR_1 \cdots R_k$ into irreducibles. Let $\ell = \operatorname{lcm}(\deg R_1, \ldots, \deg R_k)$. Then $\lambda_0^\ell(S) = S$ for all $S \in \mathbb{F}_q[z]$ with $\deg S \leq \deg R$.

Proposition

The product of all monic irreducible polynomials in $\mathbb{F}_q[z]$ with degree dividing ℓ is $z^{q^\ell} - z$.

$\mathbb{F}_{q^\ell}$ is the splitting field of $z^{q^\ell} - z$ over $\mathbb{F}_q$.
Each element in $\mathbb{F}_{q^\ell}$ has a minimal polynomial over $\mathbb{F}_q$,
so multiplying all those minimal polynomials together gives $z^{q^\ell} - z$.

R divides $1 - z^{q^\ell - 1}$, say $RT = 1 - z^{q^\ell - 1}$.
Therefore the period length of $\frac{1}{R} = \frac{T}{1 - z^{q^\ell - 1}}$ divides $q^\ell - 1$.
This can be used to show $\lambda_0^\ell(S) = S$.

Can we use the same approach modulo p^α?

Modulo p:

Theorem (slight strengthening of Engstrom 1931)

Let $R \in \mathbb{F}_p[z]$ with $R(0) \neq 0$ and $\deg R \geq 1$.
Factor $R = cR_1^{e_1} \cdots R_k^{e_k}$ into irreducibles.
Then $\frac{1}{R}$ is periodic with period length dividing $p^{\lceil \log_p e \rceil} L$
where $e = \max_{1 \leq i \leq k} e_i$ and $L = \operatorname{lcm}_{1 \leq i \leq k} (p^{\deg R_i} - 1)$.

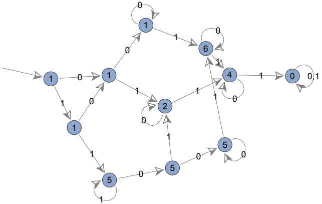
Modulo p^α:

Theorem (Engstrom 1931)

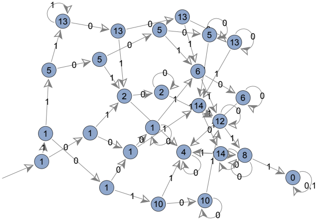
Let $R \in \mathbb{Z}/(p^\alpha \mathbb{Z})[z]$ with $r := \deg R \geq 1$ such that
the coefficients of z^0 and z^r in R are nonzero modulo p.
Then $\frac{1}{R}$ is periodic with period length dividing $p^{\alpha-1} m$
where m is the period length of $\frac{1}{R} \bmod p$.

Improved bound: $(1 + o(1)) p^{\alpha N}$ where $N = p^{2(\alpha-1)} (hd - \frac{1}{2}) + \frac{1}{2} p^{\alpha-1}$.
Singly exponential bound?

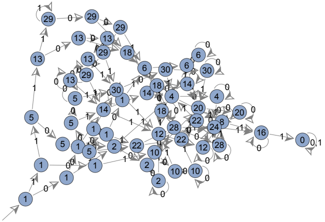
mod 8:



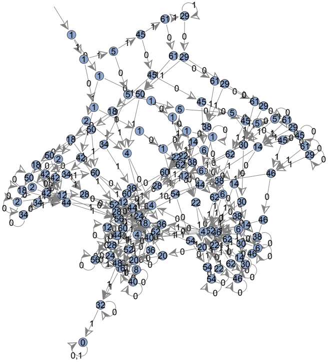
mod 16:



mod 32:



mod 64:



These automata project to each other.

So there is an inverse limit profinite automaton. Can we describe it?

$(C(n) \bmod 2)_{n \geq 0}$: $\qquad Q = (P/y \bmod 2) = xy + 1 + \frac{x}{y}$

$$\begin{aligned} S_0 &= y \\ \lambda_{0,0}(S_0) &= 0 \\ \lambda_{1,0}(S_0) &= y + 1 \end{aligned}$$

$(C(n) \bmod 4)_{n \geq 0}$: $\qquad Q = (P/y \bmod 4) = xy + 2x + 3 + \frac{x}{y}$

$$\begin{aligned} S_0 &= 2x^2y^3 + \left(2x^2 + x\right)y^2 + \left(2x^2 + 1\right)y + 2x^2 + 3x \\ \lambda_{0,0}(S_0) &= 2x^2y^2 + \left(2x^2 + 2x\right)y + 2x^2 + 2x + \tfrac{2x^2}{y} \\ \lambda_{1,0}(S_0) &= xy^2 + (x + 3)y + 3x + 1 + \tfrac{3x}{y} \end{aligned}$$

Modulo 2, these are divisible by Q.

$(C(n) \bmod 2)_{n \geq 0}$: $Q = (P/y \bmod 2) = xy + 1 + \frac{x}{y}$

$$\begin{aligned} S_0 &= y \\ \lambda_{0,0}(S_0) &= 0 \\ \lambda_{1,0}(S_0) &= y + 1 \end{aligned}$$

$(C(n) \bmod 4)_{n \geq 0}$: $Q = (P/y \bmod 4) = xy + 2x + 3 + \frac{x}{y}$

$$\begin{aligned} S_0 &= yQ + 2\left(x^2y^3 + x^2y^2 + \left(x^2 + x + 1\right)y + x^2 + x\right) \\ \lambda_{0,0}(S_0) &= 0Q + 2\left(x^2y^2 + \left(x^2 + x\right)y + x^2 + x + \frac{x^2}{y}\right) \\ \lambda_{1,0}(S_0) &= (y + 1)Q + 2\left(xy + 1 + \frac{x}{y}\right) \end{aligned}$$

Modulo 2, these are divisible by Q.

Let $D = \{0, 1, \ldots, p-1\}$.

Theorem

Every state in the automaton is of the form

$$\left(T_0 + T_1 \tfrac{p}{Q} + T_2 \left(\tfrac{p}{Q}\right)^2 + \cdots + T_{\alpha-1} \left(\tfrac{p}{Q}\right)^{\alpha-1}\right) Q^{p^{\alpha-1}-1}$$

where $T_i \in D[x, y, y^{-1}]$ for each $i \in \{0, 1, \ldots, \alpha-1\}$.

We can bound $\deg_x T_i$, $\deg_y T_i$, and $\operatorname{mindeg}_y T_i$.

Singly exponential upper bound:

$$p^N + |\mathrm{orb}_{\Lambda_0}(F)| = (1 + o(1))p^N$$

where $N = \frac{1}{6}\alpha(\alpha+1)((2hd-1)\alpha + hd + 1)$.

When $\alpha = 1$, we recover Bridy's $(1 + o(1))p^{hd}$ for $\mathbb{F}_p$.

References

- 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.
- Jan Denef and Leonard Lipshitz, Algebraic power series and diagonals, *Journal of Number Theory* **26** (1987) 46–67.
- Howard T. Engstrom, On sequences defined by linear recurrence relations, *Transactions of the American Mathematical Society* **33** (1931) 210–218.
- Harry Furstenberg, Algebraic functions over finite fields, *Journal of Algebra* **7** (1967) 271–277.
- Eric Rowland, Manon Stipulanti, and Reem Yassawi, Algebraic power series and their automatic complexity I: finite fields, `https://arxiv.org/abs/2308.10977`.