Christol's Theorem

Trevor Hyde

August 10th, 2020

Formal Laurent Series

Let $\mathbb{F}_q$ be a finite field with q elements.

Let $\mathbb{F}_q((x))$ be the field of formal Laurent series over $\mathbb{F}_q$,

$$\mathbb{F}_q((x)) := \{x^{-n}(a_0 + a_1x + a_2x^2 + \ldots) : n \geq 0, a_i \in \mathbb{F}_q\}.$$

The field $\mathbb{F}_q(x)$ of rational functions can be naturally identified with a subfield of $\mathbb{F}_q((x))$.

How do we express $f(x) \in \mathbb{F}_q(x)$ as a formal Laurent series?

Ex. Let $q = 2$.

$$\frac{x+1}{x^2+x+1} = a_0 + a_1 x + a_2 x^2 + \dots$$
$$x + 1 = (1 + x + x^2)(a_0 + a_1 x + a_2 x^2 + \dots)$$
$$= a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + (a_1 + a_2 + a_3)x^3 + \dots$$

$\therefore a_n$ satisfies a linear recurrence $a_n = a_{n-1} + a_{n-2}$ with $a_0 = 1$ and $a_1 = 0$.

$\therefore a_n$ is eventually periodic.

Theorem (Characterization of Rational Functions)

A formal Laurent series $x^{-n}(a_0 + a_1x + a_2x^2 + \ldots) \in \mathbb{F}_q((x))$ *is a rational function if and only if* (a_n) *is eventually periodic.*

Algebraic Laurent Series

$\mathbb{F}_q((x))$ is uncountable, hence most elements are transcendental over $\mathbb{F}_q(x)$.

However, there are many $f(x) \in \mathbb{F}_q((x))$ which are algebraic over $\mathbb{F}_q(x)$.

Ex. Let $f(x) \in \mathbb{F}_2((x))$ be the series $f(x) = \sum_{n \geq 0} a_n x^n$ where

$$a_n = 1 + \#\text{1's in the binary expansion of } n \bmod 2.$$

$$f(x) = 1 + x^3 + x^5 + x^6 + x^9 + \dots$$

Then $y = f(x)$ is a solution of

$$(1+x)^3 y^2 + (1+x)^2 y + x = 0.$$

Algebraic Laurent Series?

Question: How to characterize the algebraic formal Laurent series?

Christol (1979) answered this question in terms of formal series generated by *finite automata*!

q-Automatic Sequences

A sequence $(a_n) \subseteq \mathbb{F}_q$ is called *q-automatic* if there exists

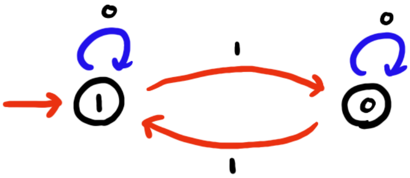
1. A finite set M with an action by the free semigroup A^*, where $A = \{0, 1, 2, \ldots, q-1\}$,
2. A *start state* $s_0 \in M$, and
3. A *dual state* $\lambda : M \to \mathbb{F}_q$,

such that if we view n as an element of A^* by expressing n in base q, then

$$a_n = \lambda(n \cdot s_0)$$

The set M with this action and extra data is called a *finite automata with output.**

Ex. The sequence
$a_n = 1 + \#1$'s in the binary expansion of n mod 2 is 2-automatic generated by the following automata.



Important Footnote*

When we encode a natural number n as a word in $\{0, 1, \ldots, q-1\}^*$ in order to define a q-automatic sequence, which direction do we read the word?

It doesn't matter!

Lemma

If (a_n) is a q-automatic sequence produced by an automata M with one reading convention, then there is another automata $\widehat{M}$ producing the same sequence with the opposite reading convention.

Theorem (Christol, 1979)

A formal power series $f(x) = \sum_{n\geq 0} b_n x^n \in \mathbb{F}_q((x))$ *is algebraic over* $\mathbb{F}_q(x)$ *if and only if* (b_n) *is a* q*-automatic sequence.*

Proof of Christol (Automatic $\longrightarrow$ Algebraic)

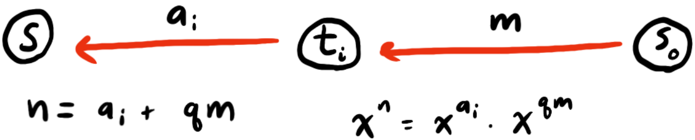
Suppose (b_n) **is** q**-automatic**, produced by the automata M.

For each state $s \in M$, let

$$f_s(x) := \sum_{\substack{n \geq 0 \\ n \cdot s_0 = s}} x^n \in \mathbb{F}_q((x)).$$

If the state t_i transitions to s under the letter a_i for $1 \leq i \leq k$, then

$$f_s(x) = \sum_{i=1}^{k} x^{a_i} f_{t_i}(x^q) = \sum_{i=1}^{k} x^{a_i} f_{t_i}(x)^q$$



Proof of Christol (Automatic $\longrightarrow$ Algebraic)

$$f_s(x) = \sum_{i=1}^{k} x^{a_i} f_{t_i}(x^q) = \sum_{i=1}^{k} x^{a_i} f_{t_i}(x)^q$$

$$f_s \in \langle f_{s_1}^q, f_{s_2}^q, \ldots, f_{s_n}^q \rangle$$

$$f_s, f_s^q \in \langle f_{s_1}^{q^2}, f_{s_2}^{q^2}, \ldots, f_{s_n}^{q^2} \rangle$$

$$\vdots$$

$$f_s, f_s^q, f_s^{q^2}, \ldots, f_s^{q^d} \in \langle f_{s_1}^{q^{d+1}}, f_{s_2}^{q^{d+1}}, \ldots, f_{s_n}^{q^{d+1}} \rangle.$$

$\Longrightarrow f_s(x)$ is algebraic over $\mathbb{F}_q(x)$ for each $s \in M$.

Hence,

$$f(x) = \sum_{n \geq 0} b_n x^n = \sum_{n \geq 0} \lambda(n \cdot s_0) x^n = \sum_{s \in M} \lambda(s) f_s(x)$$

is algebraic over $\mathbb{F}_q(x)$.

Proof of Christol (Algebraic $\longrightarrow$ Automatic)

For $0 \leq a < q$, let δ_a be the $\mathbb{F}_q$-linear operator

$$f(x) = \sum_{n \geq 0} b_n x^n \quad \xrightarrow{\delta_a} \quad \delta_a f(x) = \sum_{n \geq 0} b_{a+qn} x^n.$$

$$f(x) = \sum_{a=0}^{q-1} x^a \delta_a f(x^q) \qquad\qquad \delta_a(gf^q) = \delta_a(g)f.$$

If $w = a_0 + a_1 q + a_2 q^2 + \ldots + a_k q^k$, let

$$\delta_w = \delta_{a_k} \circ \cdots \circ \delta_{a_1} \circ \delta_{a_0}.$$

$$\delta_w f(x) = \sum_{n \geq 0} b_{w+q^{k+1}n} x^n.$$

Hence $\delta_w f(0) = b_w$.

Proof of Christol (Algebraic $\longrightarrow$ Automatic)

Let M have

- Start state $f(x)$,
- Dual state $\varepsilon : g(x) \mapsto g(0)$, and
- A^* act by $a \cdot g(x) = \delta_a g(x)$.

We have shown that this automata produces the sequence (b_n) of coefficients of $f(x)$, thus it remains to show that we can choose such an M with finitely many states.

Proof of Christol (Algebraic $\longrightarrow$ Automatic)

Suppose $f(x) \in \mathbb{F}_q((x))$ **is algebraic over** $\mathbb{F}_q(x)$**.**

Thus $\{f(x)^{q^k} : k \geq 0\}$ is linearly dependent over $\mathbb{F}_q(x)$.

$$f^{q^i} = c_1 f^{q^{i+1}} + c_2 f^{q^{i+2}} + \ldots + c_d f^{q^{i+d}}$$

$$f^{q^{i-1}} = \delta_0 f^{q^i} = (\delta_0 c_1) f^{q^i} + (\delta_0 c_2) f^{q^{i+1}} + \ldots + (\delta_0 c_d) f^{q^{i+d-1}}$$

$$\text{WLOG:} \quad f = c_1 f^q + c_2 f^{q^2} + \ldots + c_d f^{q^d},$$

with $c_i(x) \in \mathbb{F}_q[x]$.

Proof of Christol (Algebraic $\longrightarrow$ Automatic)

Let $B = \max_i \deg c_i(x)$ and let M be the $\mathbb{F}_q$-vector space spanned by $h_i(x)f(x)^{q^i}$ with $h_i(x) \in \mathbb{F}_q[x]$ of degree at most B for $0 \leq i \leq d$.

$$\delta_a(h_0 f + h_1 f^q + \ldots + h_d f^{q^d}) =$$
$$\delta_a((h_0 c_1 + h_1)f^q + \ldots + (h_0 c_d + h_d)f^{q^d}) =$$
$$\delta_a(h_0 c_1 + h_1)f + \ldots + \delta_a(h_0 c_d + h_d)f^{q^{d-1}} \in M$$

since

$$\deg \delta_a(h_0 c_i + h_i) \leq \frac{2B}{q} \leq B.$$

Therefore $\delta_a(M) \subseteq M$ for all $0 \leq a < q$.

Proof of Christol (Algebraic $\longrightarrow$ Automatic)

M is a finite dimensional vector space over $\mathbb{F}_q$, hence is a finite set.

Since $f \in M$ and M is closed under the action of A^*, it follows that M is a *finite* automata with output that produces (b_n). Therefore (b_n) is q-automatic. $\square$

Application: Transcendence Criteria

Corollary

If the coefficients of $f(x) \in \mathbb{Q}((x))$ *belong to a finite set, then either* $f(x) \in \mathbb{Q}(x)$ *or* $f(x)$ *is transcendental over* $\mathbb{Q}(x)$.

Pf: If $f(x)$ is algebraic over $\mathbb{Q}(x)$, then the reduction of f mod p is algebraic over $\mathbb{F}_p(x)$ for almost all primes p.

Christol implies that the sequence (b_n) of coefficients of $f(x)$ is p-automatic for almost all primes p.

Application: Transcendence Criteria

Hence we can choose two sufficiently large primes for which the coefficients (b_n) are all distinct modulo each prime.

Theorem (Cobham)

If (b_n) is a sequence valued in a finite set X which is q_1 and q_2 automatic for multiplicatively independent q_1 and q_2, then (b_n) is eventually periodic.

Therefore (b_n) is eventually periodic, which implies that $f(x)$ is rational. □