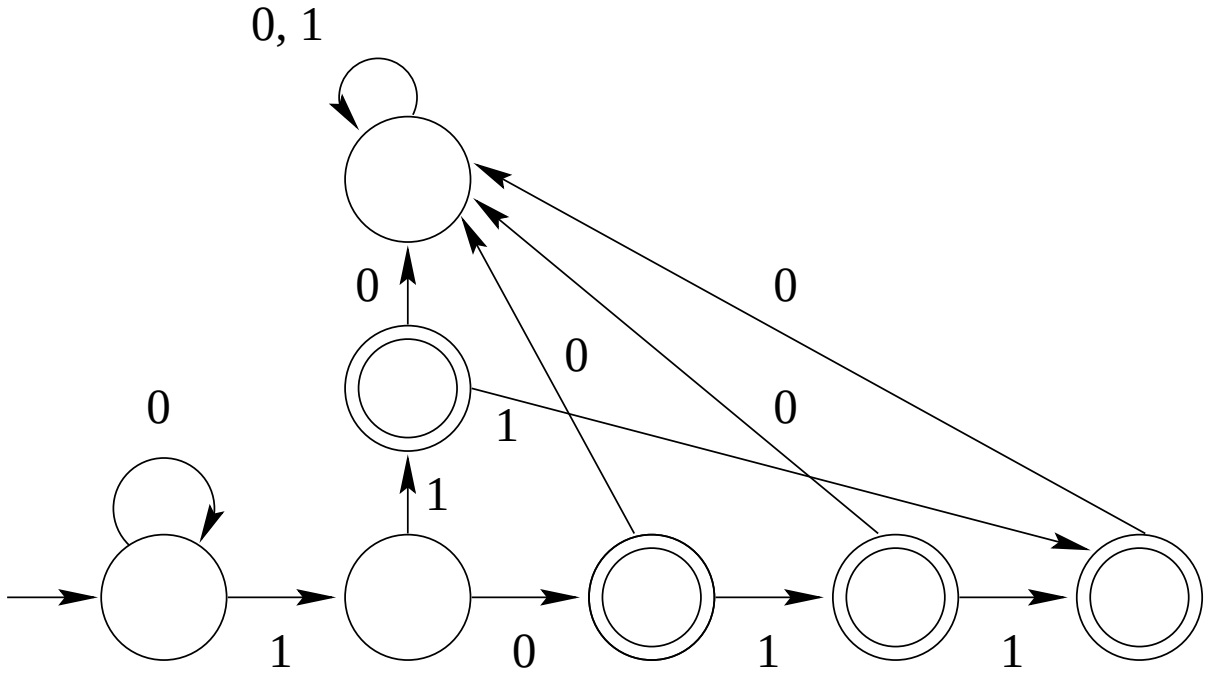
Automatic Sequences

Jeffrey Shallit
School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@graceland.uwaterloo.ca
http://www.cs.uwaterloo.ca/~shallit

Not this Waterloo!

Finite Automata

- A *deterministic finite automaton* (DFA) is a simple model of a computer.



Transition diagram for automaton accepting the base-2 representations of the primes $p \leq 11$

Basics of Finite Automata

- Formally a DFA is a quintuple: $M = (Q, \Sigma, \delta, q_0, F)$ where:
  - Q is a finite set of *states*;
  - Σ is a finite set of symbols, called the *input alphabet*;
  - $q_0 \in Q$ is the *start state*;
  - $F \subseteq Q$ is the set of *final states*;
  - $\delta : Q \times \Sigma \to Q$ is the *transition function*, which is extended to $\delta : Q \times \Sigma^*$ in the obvious way
- The *language accepted by* M is denoted by $L(M)$ and is given by

$$\{w \in \Sigma^* \mid \delta(q_0, w) \in F\}.$$

- A language L is said to be *regular* if it is accepted by some DFA M.

Automata as Computers of Sequences

- We can generalize our notion of automaton to provide an output, not simply accept/reject.
- Formally, we define a *deterministic finite automaton with output* (DFAO) as a sextuple: $(Q, \Sigma, \delta, q_0, \Delta, \tau)$, where Δ is the finite *output alphabet* and $\tau : Q \to \Delta$ is the *output mapping*.
- Next, we decide on a integer base $k \geq 2$ and represent n as a string of symbols over the alphabet $\Sigma = \{0, 1, 2, \ldots, k-1\}$.
- To compute f_n, given an automaton M, express n in base-k, say,

  $$a_r a_{r-1} \cdots a_1 a_0,$$

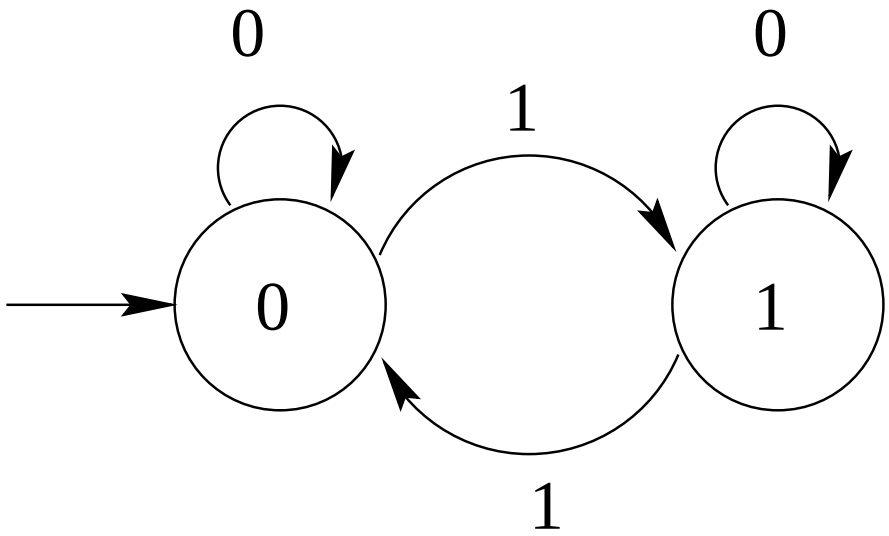
  and compute

  $$f_n = \tau(\delta(q_0, a_r a_{r-1} \cdots a_1 a_0)).$$

- Any sequence that can be computed in this way is said to be k-automatic.

Example: The Thue-Morse sequence

- The Thue-Morse sequence $(t_n)_{n\geq 0}$ is defined as follows: t_n is the parity of the number of 1's in the binary expansion of n.
- It is computed by the following DFAO:



Robustness of the Notion of Automatic Sequence

- the order in which the base-k digits are fed into the automaton in does not matter (provided it is fixed for all n);
- other representations also work (such as expansion in base-$(-k)$ using the digits $0, 1, \ldots, k-1$);
- automatic sequences are closed under many operations, such as shift, periodic deletion, q-block compression, and q-block substitution.
- if a symbol in an automatic sequence occurs with well-defined frequency r, then r is rational.

Automatic Sequences and Uniform Morphisms

The class of sequences generated by DFAO's that take their input in base k precisely corresponds to the infinite words that are images (under a coding) of iterated k-uniform morphisms.

Theorem. Let $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ be a DFAO that takes inputs in base k. Then there is a k-uniform morphism h, a letter a, and a coding r such that if the sequence $\mathbf{a} = (a_i)_{i \geq 0}$ is generated by M, then $\mathbf{a} = r(h^\omega(a))$.

Theorem

Let $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ be a DFAO that takes inputs in base k. Then there is a k-uniform morphism h, a letter a, and a coding r such that if the sequence $\mathbf{a} = (a_i)_{i \geq 0}$ is generated by M, then $\mathbf{a} = r(h^\omega(a))$.

Proof. Assume WOLOG that $\delta(q_0, 0) = q_0$.
If not, we can construct a new DFAO that generates the same sequence as follows:

- Create a new start state q_0' for which $\delta(q_0', 0) = q_0'$
- Define $\delta(q_0', a) = \delta(q_0, a)$ for $1 \leq a < k$.
- Extend τ so that $\tau(q_0') = \tau(q_0)$.

It is now easy to see that our new DFAO generates the same sequence.

Now, assuming that $\delta(q_0, 0) = q_0$, define the morphism $h : Q^* \to Q^*$ as follows:

$$h(q) = \delta(q, 0)\delta(q, 1) \cdots \delta(q, k-1).$$

Let $h^\omega(q_0) = p_0 p_1 p_2 \cdots$. Then we prove by induction on n that $\delta(q_0, (n)_k) = p_n$.

For $n = 0$, we get $\delta(q_0, (0)_k) = \delta(q_0, \epsilon) = q_0 = p_0$.

Now assume the result is true for all $n < k^i$; we prove the result for $k^i \leq n < k^{i+1}$.

Write $(n)_k = n_1 n_2 \cdots n_{i+1}$.

Let $m = [n_1 \cdots n_i]_k$, that is, the integer represented in base-k by $n_1 \cdots n_i$, so that $n = km + n_{i+1}$.

Then

$$\begin{aligned}
\delta(q_0, (n)_k) &= \delta(q_0, n_1 n_2 \cdots n_{i+1}) \\
&= \delta(\delta(q_0, n_1 \cdots n_i), n_{i+1}) \\
&= \delta(p_m, n_{i+1}) \\
&= (h(p_m))[n_{i+1}] \\
&= p_{km+n_{i+1}} \\
&= p_n.
\end{aligned}$$

Now let $r = \tau$ and $a = q_0$. We then have $r(h^\omega(a)) = \mathbf{a}$. The proof is complete.

The Other Direction

Theorem

Let $\tau(h^\omega(a)) = \mathbf{a} = a_0 a_1 a_2 \cdots$ *for a* k*-uniform morphism*

$$h : \Sigma^* \to \Sigma^*$$

and a coding $\tau : \Sigma \to \Delta$*. Then* $\mathbf{a}$ *is generated by a* k*-automaton.*

Proof.

Define

- $M = (Q, \{0, 1, \ldots, k-1\}, \delta, q_0, \Delta, \tau)$, where
- $Q = \Sigma$,
- $q_0 = a$,
- $\delta(q, i) = (h(q))[i]$ for each $q \in Q$ and $0 \leq i < k$.

An easy proof by induction, similar to that of the previous theorem, completes the proof.

The Rudin-Shapiro Sequence

The Rudin-Shapiro sequence $(r_n)_{n\geq 0}$, is defined as follows: r_n is 1 (resp. -1) according to whether the number of (possibly overlapping) occurrences of "11" in the binary expansion of n is even (resp. odd).
Then $(r_n)_{n\geq 0}$ is 2-automatic, since it is generated by the DFAO below

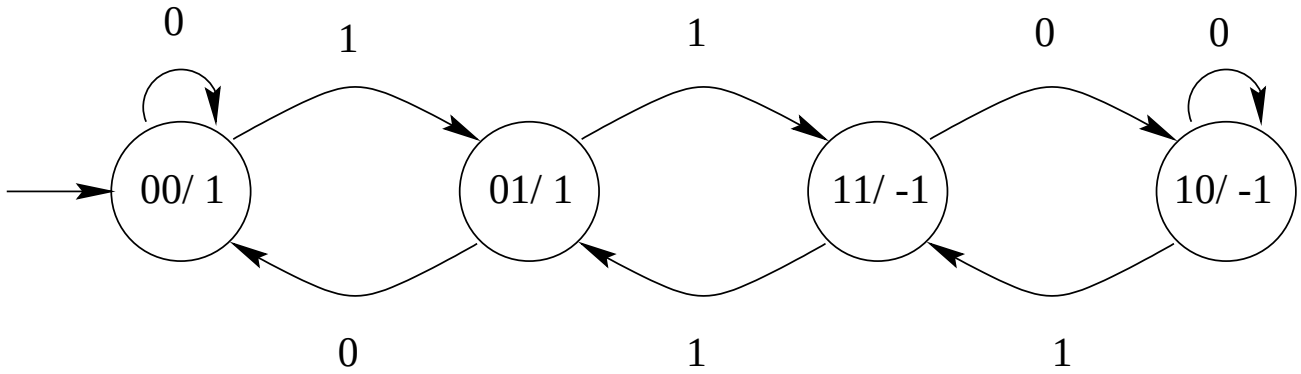


Figure: DFAO generating the Rudin-Shapiro sequence

Here the meaning of a state labeled ab/c is that the running sum of the number of occurrences of "11" so far is congruent to a modulo 2, the last digit input was b, and the output is c.

The Rudin-Shapiro Sequence

Here is another interesting feature of the Rudin-Shapiro sequence. Suppose we consider a path visiting lattice points in the plane. We start at the origin and make a first move to $(0, 1)$. At step n, for $n \geq 1$, we decide to turn left (L) or right (R) according to the following rule:

$$d_n = \begin{cases} \mathtt{L}, & \text{if } r_n r_{n-1} = (-1)^n; \\ \mathtt{R}, & \text{if } r_n r_{n-1} = -(-1)^n. \end{cases} \tag{1}$$

The first few terms of this sequence are given below:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
r_n	1	1	1	-1	1	1	-1	1	1	1	1	-1	-1	-1	...
d_n		R	L	L	R	R	R	L	L	R	L	L	L	R	...

We then get a space-filling curve that visits every lattice point in the $\frac{1}{8}$ of the plane; see the picture on the next slide.

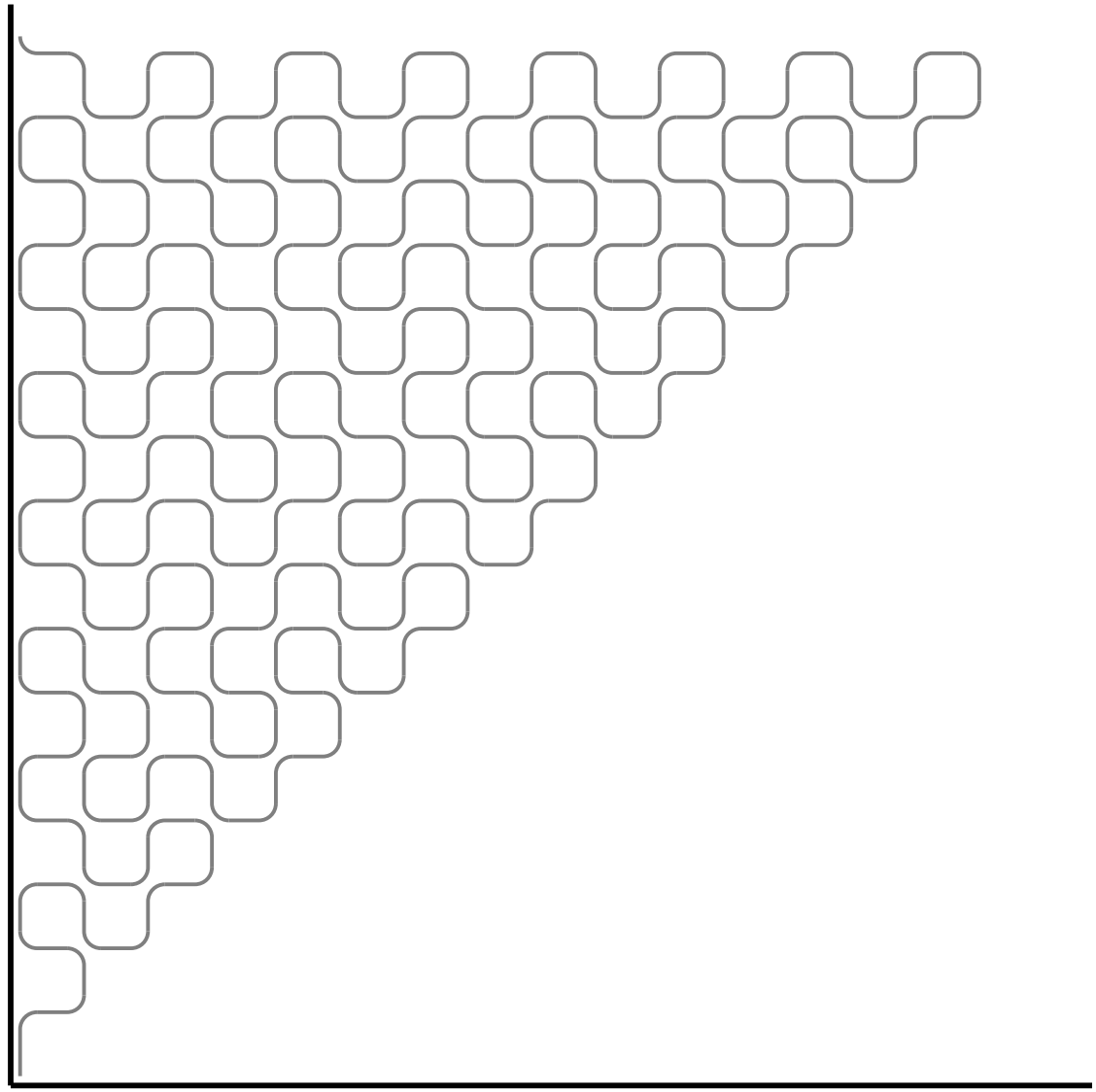


Figure: Space-filling curve derived from the Rudin-Shapiro sequence

An Open Problem

It is not hard to show that the curve corresponding to the Rudin-Shapiro sequence is self-avoiding.

One can consider similar curves where 11 is replaced by another string of digits.

It is not hard to show that in all cases except 00, 11, and 1^k0, 0^k1, $k \geq 1$, the resulting curves are self-intersecting.

However, no proof is known that the curves are self-avoiding for 1^k0, 0^k1 for $k \geq 2$.

The k-Kernel

There is yet another characterization of the automatic sequences in terms of the k-kernel.

Let

$$\mathbf{a} = a_0 a_1 a_2 \cdots$$

be an infinite sequence.

The k-kernel is the set of sequences of the form

$$\{(a_{k^i n+c})_{n\geq 0} \ : \ i \geq 0, \ 0 \leq c < k^i\}.$$

Theorem

The sequence $\mathbf{a}$ *is* k*-automatic if and only its* k*-kernel is finite.*

The k-Kernel

Exercise. Give an example of a sequence over $\{0, 1\}$ such that every element of the 2-kernel is distinct.

Exercise. Show that the sequence generated by iterating the morphism defined by $\mathtt{a} \to \mathtt{aab}$, $\mathtt{b} \to \mathtt{b}$, is not 2-automatic.

Open Problem. Consider the morphism defined by

$$\begin{aligned} 1 &\to 121 \\ 2 &\to 12221 \end{aligned}$$

and the fixed point

$$\mathbf{d} = d_0 d_1 d_2 \cdots = 12112221 \cdots .$$

Then $d(64n) = d(16n)$ for $0 \leq n < 119304647$, but $d(64n) \neq d(16n)$ for $n = 119304647$. Develop a complete explanation of this kind of behavior.

Closure Properties of Automatic Sequences

What transformations on automatic sequences we can perform and still get an automatic sequence?

In finding and proving these properties, we have three different characterizations we can use:

- fixed points of k-uniform morphisms;
- sequences generated by k-automata; or
- sequences with a finite k-kernel.

Some properties are easier to prove using one representation than another, and you should try several different approaches when encountering a new property.

Closure Properties of Automatic Sequences

Theorem

Let $\mathbf{a} = a_0 a_1 a_2 \ldots$ *and* $\mathbf{b} = b_0 b_1 b_2 \ldots$ *be two* k*-automatic sequences taking values in* Γ *and* Δ*, respectively.*
Let $f : \Gamma \times \Delta \to \Lambda$ *be a function.*
Then the sequence $f(\mathbf{a}, \mathbf{b}) = (f(a_i, b_i))_{i \geq 0}$ *is* k*-automatic.*

Proof. Since **a** and **b** are k-automatic, they are generated by k-uniform morphisms and codings; let us say

$$\mathbf{a} = \rho(g^\omega(c))$$

and

$$\mathbf{b} = \tau(h^\omega(d)).$$

Define $g(r) = r'_1 \cdots r'_k$ and $h(s) = s'_1 \cdots s'_k$.

Now define a new morphism

$$G([r, s]) = [r'_1, s'_1] \cdots [r'_k, s'_k].$$

Clearly G is k-uniform.

Define the coding

$$\xi([r,s]) = f(\rho(r), \tau(s)).$$

Then it is easy to verify that

$$f(\mathbf{a}, \mathbf{b}) = \xi(G^{\omega}([c,d])).$$

Closure Properties of Automatic Sequences

Theorem

Let r be any integer ≥ 1. The sequence $\mathbf{a}$ is k-automatic if and only if it is k^r-automatic.

Proof. First, let's show that if $\mathbf{a}$ is k-automatic, then it is k^r-automatic. This is easiest using the representation as image of a fixed point of a k-uniform morphism.

Since $\mathbf{a}$ is k-automatic, we can write it as

$$\mathbf{a} = \tau(h^\omega(a))$$

for some coding τ, prolongable k-uniform morphism h, and letter a. Now let $g = h^r$. Clearly g is k^r-uniform, and $\mathbf{a} = \tau(g^\omega(a))$.

Closure Properties of Automatic Sequences

The other direction has an easy proof using automata. Given a k^r-automaton generating **a**, how do we create a k-automaton generating the same string?
For each state q, we erect a complete k-ary tree rooted at $q = q_\epsilon$, containing

$$k + k^2 + \cdots + k^r$$

new states, labeled q_w for $0 < |w| < r$. We define a new transition function δ' such that

$$\delta'(q_w, a) = q_{wa}$$

for $0 \leq |w| < r - 1$, and

$$\delta'(q_x, a) = \delta(q, [xa]_k)$$

for $|x| = r - 1$. We also define $\tau(q_w) = \tau(\delta(q, [w]_k))$. This new machine generates **a**.

Convolution of Automatic Sequences

Let's look at an example of a closure property where a proof using the k-kernel seems easiest.

Consider a finite additively-commutative semiring R with operations $+$ and $\cdot$, and let $\mathbf{a} = (a_i)_{i \geq 0}$ and $\mathbf{b} = (b_i)_{i \geq 0}$ be sequences taking values in R.
Define the *convolution* of $\mathbf{a}$ with $\mathbf{b}$ (written $\mathbf{a} \star \mathbf{b}$) as the sequence $(c_i)_{i \geq 0}$ where

$$c_n = \sum_{0 \leq i \leq n} a_i b_{n-i}.$$

Theorem

If $\mathbf{a}$, $\mathbf{b}$ *are* k*-automatic sequences, then so is* $\mathbf{a} \star \mathbf{b}$.

Convolution of Automatic Sequences

Proof. Define $\mathbf{c} = \mathbf{a} \star \mathbf{b} = (c_i)_{i \geq 0}$.
Since $\mathbf{a}$ and $\mathbf{b}$ are k-automatic, their k-kernels are finite.
We will show that the k-kernel of $\mathbf{c}$ is finite, too.
Write

$$\mathbf{A}_{e,s} = (a_{k^e n+s})_{n \geq 0}$$

and

$$\mathbf{B}_{f,t} = (b_{k^f n+t})_{n \geq 0}.$$

Convolution of Automatic Sequences

Then

$$c_{k^g n+d} = \sum_{0\le i\le d} (\mathbf{A}_{g,i} \star \mathbf{B}_{g,d-i})[n] + \sum_{d<g<k^g} (\mathbf{A}_{g,j} \star \mathbf{B}_{g,k^g+d-j})[n-1]. \quad (2)$$

To verify this, note that the n'th term of $\mathbf{A}_{g,i} \star \mathbf{B}_{g,d-i}$ contains terms of the form

$$a_{k^g(n-l)+i}\ b_{k^g l+d-i}$$

for $0 \le l \le n$, and the $n-1$'th term of

$$\mathbf{A}_{g,j} \star \mathbf{B}_{g,k^g+d-j}$$

is either 0 (if $n = 0$) or contains terms of the form

$$a_{k^g(n-1-l)+j}\ b_{k^g l+k^g+d-j}$$

for $0 \le l \le n-1$.

In both cases the sum of the indices is $k^g n + d$, as desired, and these terms are evidently distinct, as the indices of a are distinct (mod k^g).

Finally, the total number of the terms being summed is $(n+1)(d+1) + n(k^g - d - 1) = nk^g + d + 1$, so each term making up $c_{k^g n+d}$ is accounted for exactly once.

Although it may not appear useful at first glance, equation (3) is the key to showing that the k-kernel of $\mathbf{c}$ is finite. For each $\mathbf{A}_{g,i}$ is actually one of the elements of the k-kernel of $\mathbf{a}$, and each $\mathbf{B}_{e,f}$ is one of the elements of the k-kernel of $\mathbf{b}$.

Let

$$\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_p$$

be the sequences in the k-kernel of $\mathbf{a}$, and let

$$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_q$$

be the sequences in the k-kernel of $\mathbf{b}$.

Now define $\mathbf{u}_{i,j} = \mathbf{a}_i \star \mathbf{b}_j$ for $1 \leq i \leq p$, $1 \leq j \leq q$.

Also let $\mathbf{u}_{i,j} = (u_{i,j}(n))_{n \geq 0}$ and define $\mathbf{v}_{i,j} = (v_{i,j}(n))_{n \geq 0}$ where

$$v_{i,j}(n) = \begin{cases} 0, & \text{if } n = 0; \\ u_{i,j}(n-1), & \text{if } n \geq 1; \end{cases}$$

Convolution of Automatic Sequences

Thus any subseqence $(c_{k^g n+d})_{n\geq 0}$ is the sum of a finite number of elements of the sequences $\mathbf{u}_{i,j}$ and $\mathbf{v}_{i,j}$.

Since all our sequences take their values in a finite semiring, however, there are only finitely many different sequences of the form $t\mathbf{u}_{i,j}$ and $t\mathbf{v}_{i,j}$ where t ranges over all integers, and hence an arbitrary non-negative integer linear combination of the $\mathbf{u}_{i,j}$ and $\mathbf{v}_{i,j}$ can result in only finitely many distinct sequences.

It follows that the k-kernel of $\mathbf{c}$ is finite.

Closure Properties of Automatic Sequences

Exercise. Show that if $(c(n))_{n\geq 0}$ is a k-automatic sequence, and a and b are non-negative integers, then $(c(an+b))_{n\geq 0}$ is k-automatic. Part of the problem is determining which representation of k-automatic sequences is easiest to use here.

Formal Power Series

Recall the definitions of formal power series and formal Laurent series.
The ring $K[[X]]$ of formal power series with coefficients in a field K is defined by

$$K[[X]] := \left\{ \sum_{n \geq 0} a_n X^n \ : \ a_n \in K \right\},$$

where

$$\left(\sum_{n \geq 0} a_n X^n \right) + \left(\sum_{n \geq 0} b_n X^n \right) := \sum_{n \geq 0} (a_n + b_n) X^n$$

Formal Power Series

and

$$\left(\sum_{n\geq 0} a_n X^n\right) \times \left(\sum_{n\geq 0} b_n X^n\right) := \sum_{n\geq 0}\left(\sum_{i+j=n} a_i b_j\right) X^n.$$

The ring $K[[X]]$ is a subring of the field $K((X))$ of formal Laurent series defined by

$$K((X)) = \left\{ \sum_{n\geq -n_0} a_n X^n \ : \ n_0 \in \mathbb{Z},\ a_n \in K \right\},$$

where the addition and the multiplication are defined in a similar way.

Since this field contains the field of rational functions $K(X)$, we can define algebraicity over $K(X)$.

We recall that a formal Laurent series

$$F(X) = \sum_{n \geq -n_0} a_n X^n$$

is said to be algebraic over the field $K(X)$, or just algebraic, if there exist an integer $d \geq 1$ and polynomials $A_0(X)$, $A_1(X)$, ..., $A_d(X)$, with coefficients in K and not all zero, such that

$$A_0 + A_1 F + A_2 F^2 + \cdots + A_d F^d = 0.$$

Example: The (Misnamed) Fredholm Series

Let f be the formal power series on $GF(2)$ defined by

$$f(X) = X + X^2 + X^4 + \cdots = \sum_{i \geq 0} X^{2^i}.$$

This series is algebraic over $GF(2)(X)$, since

$$f(X^2) = f(X) - X,$$

which implies, over $GF(2)$, that

$$f(X)^2 + f(X) + X = 0.$$

This series f is sometimes called the Fredholm series, but Fredholm apparently never studied it.

The Thue-Morse Power Series

Let $T(X) = \sum_{n \geq 0} t_n X^n$ where $(t_n)_{n \geq 0}$ is the Thue-Morse sequence. Then

$$T(X) = X + X^2 + X^4 + X^7 + X^8 + X^{11} + \cdots$$

Yesterday we showed that $T(X^{-1})$ is quadratic, and so $T(X)$ is also.

Generalized Thue-Morse Power Series

Generalizing the previous example, let p be a prime number, let $t_p(n) = s_p(n) \bmod p$, where $s_p(n)$ denotes the sum of the bits of n when expressed in base p. Let $T_p(X) = \sum_{n \geq 0} t_p(n) X^n$.
Then we have

$$\begin{aligned} T_p(X) &= \sum_{0 \leq a < p} \sum_{n \geq 0} t_p(pn + a) X^{pn+a} \\ &= \sum_{0 \leq a < p} \sum_{n \geq 0} (t_p(n) + a) X^{pn+a} \\ &= \left(\sum_{0 \leq a < p} X^a T_p(X)^p \right) + \left(\sum_{0 \leq a < p} a X^a (\sum_{n \geq 0} X^n)^p \right) \end{aligned}$$

So

$$\left(\sum_{0\le a<p} X^a T_p(X)^p\right) + \left(\sum_{0\le a<p} aX^a (\sum_{n\ge 0} X^n)^p\right)$$

$$\begin{aligned}
&= T_p(X)^p \left(\sum_{0\le a<p} X^a\right) + \\
&\quad \frac{1}{(1-X)^p}\left(\sum_{0\le a<p} aX^a\right) \\
&= T_p(X)^p \ \frac{1-X^p}{1-X} + \frac{1}{(1-X)^p}\cdot\frac{X(1-X)^p}{(X-1)^2} \\
&= T_p(X)^p \ \frac{1-X^p}{1-X} + \frac{X}{(1-X)^2}.
\end{aligned}$$

It follows that

$$(1-X)^{p+1}T_p(X)^p - (1-X)^2 T_p(X) + X = 0,$$

which proves that T_p is algebraic over $GF(p)(X)$.

Exercise. Prove that

$$(1-X)^{p+1}Y^p - (1-X)^2 Y + X$$

is irreducible.

Christol's Theorem

Let's generalize the preceding examples.

First, let's define operators on the formal power series and prove two lemmas.

We define, for $0 \leq r < q$, a linear transformation

$$\Lambda_r : GF(q)[[X]] \to GF(q)[[X]]$$

as follows:

$$\Lambda_r \left(\sum_{i \geq 0} a_i X^i \right) = \sum_{i \geq 0} a_{qi+r} X^i.$$

Note that, if p is a polynomial, then

$$\deg \Lambda_r(p) \leq \frac{\deg p}{q}.$$

Christol's Theorem

Lemma. (a) Let A be a formal power series in $GF(q)[[X]]$. Then

$$A(X) = \sum_{i \geq 0} a_i X^i = \sum_{0 \leq r < q} X^r \Lambda_r(A(X))^q. \tag{3}$$

Proof. (a)

$$A(X) = \sum_{i \geq 0} a_i X^i = \sum_{0 \leq r < q} \sum_{i \geq 0} a_{qi+r} X^{qi+r}$$

$$= \sum_{0 \leq r < q} X^r \sum_{i \geq 0} a_{qi+r} X^{iq}.$$

Hence

$$A(X) = \sum_{0 \leq r < q} X^r \left(\sum_{i \geq 0} a_{qi+r} X^i \right)^q$$

$$= \sum_{0 \leq r < q} X^r \Lambda_r(A(X))^q.$$

(b) Let G and H be two formal power series in $GF(q)[[X]]$. Then

$$\Lambda_r(G^q H) = G\Lambda_r(H). \tag{4}$$

Proof.

$$\begin{aligned}
\Lambda_r(G^q H) &= \Lambda_r\left(\left(\sum_{k\geq 0} g_k X^k\right)^q \left(\sum_{j\geq 0} h_j X^j\right)\right) \\
&= \Lambda_r\left(\left(\sum_{k\geq 0} g_k X^{qk}\right) \left(\sum_{j\geq 0} h_j X^j\right)\right) \\
&= \Lambda_r\left(\sum_{i\geq 0} X^i \sum_{\substack{k,j\geq 0 \\ qk+j=i}} g_k h_j\right).
\end{aligned}$$

$$
\begin{aligned}
\Lambda_r\left(\sum_{i\geq 0} X^i \sum_{\substack{k,j\geq 0\\ qk+j=i}} g_k h_j\right) &= \sum_{i\geq 0} X^i \left(\sum_{\substack{k,j\geq 0\\ qk+j=qi+r}} g_k h_j\right)\\
&= \sum_{i\geq 0} X^i \left(\sum_{0\leq k\leq i} g_k h_{q(i-k)+r}\right)\\
&= \sum_{k\geq 0} g_k X^k \left(\sum_{i\geq k} h_{q(i-k)+r} X^{i-k}\right)\\
&= \sum_{k\geq 0} g_k X^k \left(\sum_{i\geq 0} h_{qi+r} X^i\right)
\end{aligned}
$$

$$\begin{aligned}\Lambda^r(G^q H) &= \left(\sum_{k\geq 0} g_k X^k\right)\left(\sum_{i\geq 0} h_{qi+r} X^i\right)\\ &= G\cdot\Lambda_r(H).\end{aligned}$$

Christol's Theorem

Lemma. Let $F(X) = \sum_{i \geq 0} a_i X^i$ be a formal power series with coefficients in $GF(q)$, where $q = p^n$. Then F is algebraic over $GF(q)(X)$ if and only if there exist an integer $t \geq 0$ and $t+1$ polynomials $B_0(X), \ldots, B_t(X)$, not all equal to zero, such that

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0.$$

Furthermore we can suppose that $B_0 \neq 0$.

Proof. If F is algebraic, the series F, F^q, F^{q^2}, ..., cannot be all linearly independent. Hence there exists a nontrivial linear relation

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0.$$

On the other hand if such a nontrivial relation holds, the series F is clearly algebraic.

Now let us prove that we can find such a relation with $B_0 \neq 0$.
Assume that

$$B_0 F + B_1 F^q + B_2 F^{q^2} + \cdots + B_t F^{q^t} = 0$$

with t minimal, and let j be the smallest non-negative integer such that $B_j(X) \neq 0$.
We show that $j = 0$.
Since

$$B_j = \sum_{0 \leq r < q} X^r (\Lambda_r(B_j))^q$$

by (3), it follows that there exists an r with $\Lambda_r(B_j) \neq 0$.

Now, since $\sum_{j\leq i\leq t} B_i F(X)^{q^i} = 0$, we have

$$\sum_{j\leq i\leq t} \Lambda_r(B_i F^{q^i}) = 0$$

and, using our Lemma that says $\Lambda_r(G^q H) = G\Lambda_r(H)$, we see that, if $j \neq 0$,

$$\sum_{j\leq i\leq t} \Lambda_r(B_i) F^{q^{i-1}} = 0,$$

which gives a new relation with the coefficient of $F^{q^{j-1}} \neq 0$, a contradiction, hence $j = 0$.
We thus have the relation

$$\sum_{0\leq i\leq t} B_i F^{q^i} = 0,$$

with $B_0 \neq 0$.

Christol's Theorem

Lemma. Suppose $\mathbf{a} = (a_i)_{i \geq 0}$ is a sequence over $GF(q)$. Then $\mathbf{a}$ is q-automatic if and only if there exists a finite collection of formal power series $\mathcal{F}$ such that (a) $f \in \mathcal{F}$, where $f(X) := \sum_{i \geq 0} a_i X^i$; and (b) for all $g \in \mathcal{F}$, $0 \leq r < q$, we have $\Lambda_r(g) \in \mathcal{F}$.

Proof. Let $K_q(\mathbf{a}) = \{\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \ldots, \mathbf{a}^{(r)}, \ldots\}$ be the q-kernel of the sequence $\mathbf{a}$, with $\mathbf{a} = \mathbf{a}^{(1)}$.
Write $\mathbf{a}^{(i)} = (a_n^{(i)})_{n \geq 0}$.
($\Longrightarrow$): Take

$$\mathcal{F} = \left\{ \sum_{n \geq 0} a_n^{(i)} X^n \ : \ 1 \leq i \leq r \right\}.$$

($\Longleftarrow$): We have $\sum_{n\geq 0} a_n^{(i)} X^n \in \mathcal{F}$. It follows that $|K_q(\mathbf{a})| \leq |\mathcal{F}|$, so the q-kernel is finite.

Christol's Theorem

Theorem (Christol). Let Δ be a (non-empty) finite set, and let $\mathbf{a} = (a_i)_{i \geq 0}$ be a sequence over Δ. Let p be a prime number. Then $\mathbf{a}$ is p-automatic if, and only if, there exists an integer $n \geq 1$ and an injective map $\beta : \Delta \to GF(p^n)$ such that the formal power series $\sum_{i \geq 0} \beta(a_i) X^i$ is algebraic over $GF(p^n)(X)$.

Proof. ($\Longrightarrow$): Choose an integer n sufficiently large such that $|\Delta| \leq p^n$, and an injection $\beta : \Delta \to GF(p^n)$. We may therefore assume, without loss of generality that $\Delta \subseteq GF(p^n)$.
Let us then show that $\sum_{i \geq 0} a_i X^i$ is algebraic over $GF(p^n)(X)$.
Since $(a_i)_{i \geq 0}$ is p-automatic, we know from a previous theorem that it is q-automatic where $q = p^n$. By another theorem we know that the q-kernel $K_q(\mathbf{a})$ is finite, say $K_q(\mathbf{a}) = \{\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \ldots, \mathbf{a}^{(d)}\}$, with $\mathbf{a}^{(1)} = \mathbf{a}$. Write $\mathbf{a}^{(i)} = (a_n^{(i)})_{n \geq 0}$. Define

$$F_j(X) = \sum_{n \geq 0} a_n^{(j)} X^n \quad \text{for } 1 \leq j \leq d.$$

Then, for $1 \leq j \leq d$

$$\begin{aligned} F_j(X) &= \sum_{0 \leq r \leq q-1} \sum_{m \geq 0} a^{(j)}_{qm+r} X^{qm+r} \\ &= \sum_{0 \leq r \leq q-1} X^r \sum_{m \geq 0} a^{(j)}_{qm+r} X^{qm}. \end{aligned}$$

But the sequence $(a^{(j)}_{qm+r})_{m \geq 0}$ is one of the $a^{(i)}$'s, which shows that $F_j(X)$ is a $GF(q)[X]$-linear combination of the power series $F_i(X^q)$. In other words $F_j(X)$ belongs to the $GF(q)(X)$-vector space generated by the series $F_i(X^q)$:

$$F_j(X) \in \langle F_1(X^q), F_2(X^q), \ldots, F_d(X^q) \rangle$$

for $1 \leq j \leq d$.

But this implies that

$$F_j(X^q) \in \langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2}) \rangle,$$

for $1 \leq j \leq d$, and also, by transitivity, that

$$F_j(X) \in \langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2}) \rangle$$

for $1 \leq j \leq d$.
Hence both $F_j(X)$ and $F_j(X^q)$ are in

$$\langle F_1(X^{q^2}), F_2(X^{q^2}), \ldots, F_d(X^{q^2}) \rangle$$

for $1 \leq j \leq d$.

This implies that $F_j(X^q)$ and $F_j(X^{q^2})$ are in

$$\langle F_1(X^{q^3}), F_2(X^{q^3}), \ldots, F_d(X^{q^3})\rangle$$

for $1 \leq j \leq d$.
Hence $F_j(X)$, $F_j(X^q)$, and $F_j(X^{q^2})$ are in

$$\langle F_1(X^{q^3}), F_2(X^{q^3}), \ldots, F_d(X^{q^3})\rangle$$

for $1 \leq j \leq d$.
Iterating, we get

$$F_j(X^{q^k}) \in \langle F_1(X^{q^{d+1}}), F_2(X^{q^{d+1}}), \ldots, F_d(X^{q^{d+1}})\rangle$$

for $1 \leq j \leq d$, $0 \leq k \leq d$.

But the dimension of

$$\langle F_1(X^{q^{d+1}}), F_2(X^{q^{d+1}}), \ldots, F_d(X^{q^{d+1}})\rangle$$

as a vector space over $GF(q)(X)$ is at most d, the number of generators.
So for $1 \leq j \leq d$, the formal power series

$$F_j(X), F_j(X^q), \ldots, F_j(X^{q^d})$$

are linearly related over $GF(p^n)(X)$.

In particular for $j = 1$, this gives that $F_1(X) = \sum_{i\geq 0} a_i^{(1)} X^i$ is algebraic over $GF(p^n)(X)$.

The Other Direction

($\Longleftarrow$): Suppose that $F(X) = \sum_{i \geq 0} a_i X^i$ is algebraic over $GF(q)(X)$.
Then there exist polynomials $B_0(X), \ldots, B_t(X)$ such that

$$\sum_{0 \leq i \leq t} B_i(X) F(X)^{q^i} = 0,$$

and $B_0 \neq 0$.

Put $G = \frac{F(X)}{B_0(X)}$; then

$$G = \sum_{1 \leq i \leq t} C_i G^{q^i} \quad \text{where } C_i = -B_i B_0^{q^i - 2}.$$

Now let

$$N = \max(\deg B_0, \max_i \deg C_i)$$

and let $\mathcal{H}$ be defined as follows:

$$\mathcal{H} = \{H \in GF(q)[[X]] : H = \sum_{0 \le i \le t} D_i G^{q^i}$$

$$\text{with } D_i \in GF(q)[X] \text{ and } \deg D_i \le N\}.$$

Now $\mathcal{H}$ is a finite set and $F = B_0 G$ belongs to $\mathcal{H}$.

We now show that $\mathcal{H}$ is mapped into itself by Λ_r.
Let $H \in \mathcal{H}$. Then

$$\begin{aligned}
\Lambda_r(H) &= \Lambda_r\left(D_0 G + \sum_{1\le i\le t} D_i G^{q^i}\right) \\
&= \Lambda_r\left(\sum_{1\le i\le t} (D_0 C_i + D_i) G^{q^i}\right) \\
&= \sum_{1\le i\le t} \Lambda_r(D_0 C_i + D_i) G^{q^{i-1}}
\end{aligned}$$

Since $\deg D_0, \deg D_i, \deg C_i \le N$, it follows that $\deg(D_0 C_i + D_i) \le 2N$, and so

$$\deg(\Lambda_r(D_0 C_i + D_i)) \le \frac{2N}{q} \le N.$$

By a previous lemma, the sequence $(a_i)_{i\ge 0}$ is q-automatic.

Application of Christol's Theorem

Here we give one application of Christol's theorem. (Further applications to transcendence will be covered by Jean-Paul Allouche in his lectures.)

Suppose $F = \sum_{i \geq 0} f_i X^i$ and $G = \sum_{i \geq 0} g_i X^i$ are two formal power series in $K[[X]]$. The Hadamard product is defined to be

$$F \odot G = \sum_{i \geq 0} f_i g_i X^i.$$

Theorem. If F, G are algebraic over $GF(q)(X)$, then so is $F \odot G$.

Proof. Suppose F and G are algebraic over $GF(q)(X)$. Then, by Christol's theorem, the sequences $(f_i)_{i \geq 0}$ and $(g_i)_{i \geq 0}$ are q-automatic.
Then, by Theorem 4, the sequence $(f_i g_i)_{i \geq 0}$ is q-automatic.
Hence, by Christol's theorem, $F \odot G$ is algebraic over $GF(q)(X)$.

Application of Christol's Theorem

Notice this theorem is not true, in general, for characteristic 0. For example,

$$F = \sum_{n \geq 0} \binom{2n}{n} X^n = (1 - 4X)^{-1/2}$$

is algebraic over any field K, but it can be shown that $F \odot F$ is transcendental over $\mathbb{Q}(X)$.