WHAT IS...

an Automatic Sequence?

Eric Rowland

A sequence $s(n)_{n\geq 0}$ is called *k-automatic* if $s(n)$ is a finite-memory function of the base-k digits of n. This means that some computer with only finitely many possible states can compute $s(n)$ for any n by reading the base-k digits of n one at a time (beginning with the least significant digit) and following a transition rule that specifies the next state of the computer as a function of both the current state and the current digit being read. Each possible state of the computer has an associated output value, and the result of the computation is the output value corresponding to the state of the computer after it has read the final digit. A computer of this kind is called an *automaton*, hence the name "automatic sequence."

For example, consider an automaton with only two states, q_1 and q_2, that reads binary representations of integers. Suppose the automaton starts in state q_1 and performs transitions according to the function $\delta : \{q_1, q_2\} \times \{0, 1\} \to \{q_1, q_2\}$ given by the following table.

δ	0	1
q_1	q_1	q_2
q_2	q_2	q_1

Let the output function $\tau : \{q_1, q_2\} \to \{a, b\}$ be given by $\tau(q_1) = a$ and $\tau(q_2) = b$. The first few terms of $s(n)_{n\geq 0}$ are as follows.

n	0	1	2	3	4	5	6	7
$s(n)$	a	b	b	a	b	a	a	b

Eric Rowland is a Marie Curie Actions COFUND postdoctoral fellow at the University of Liège. His email address is `rowland@lacim.ca`.

DOI: http://dx.doi.org/10.1090/noti1218

For example, the standard binary representation of $n = 0$ is the empty word; to compute $s(0)$ the automaton starts in state q_1, performs no transitions, and outputs $\tau(q_1) = a$. When fed the binary digits of $n = 1 = 1_2$, the output of the automaton is

$$s(1) = \tau(\delta(q_1, 1)) = \tau(q_2) = b.$$

For $n = 2 = 10_2$, we get

$$s(2) = \tau(\delta(\delta(q_1, 0), 1)) = \tau(q_2) = b,$$

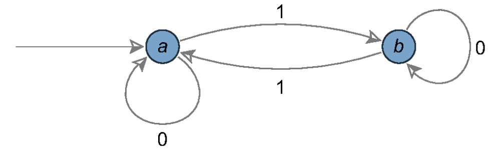
etc. To compute the value of $s(n)$, the automaton performs approximately $\log_2 n$ transitions.

The sequence

$$s(n)_{n\geq 0} = a, b, b, a, b, a, a, b, b, a, a, b, a, b, b, a, \ldots$$

is known as the Thue–Morse sequence. It is 2-automatic, since we are reading integers in base 2. Reading the least significant digit first is only a convention, since reading in the other direction turns out to give the same class of sequences.

It is illustrative to identify an automaton with a directed graph. We create a vertex for each state, and labeled edges encode the transition function δ. An unlabeled edge identifies the initial state, and each state is labeled with its output value. The automaton for the Thue–Morse sequence is the following:



We can compute $s(n)$ from the graph by starting in q_1 and following edges labeled with successive binary digits of n.

Since an automaton has only finitely many states, an automatic sequence is a sequence on a finite alphabet; and among sequences on finite alphabets, the class of automatic sequences is quite fundamental. There is no class known with more descriptive power and as many major properties. Automatic sequences generalize periodic sequences in the sense that each periodic sequence is k-automatic for all $k \geq 2$. In particular, this implies there is a "divisibility rule" for every integer in every base.

Automatic Sequences in Combinatorics

The structure of a k-automatic sequence reflects the recursive structure of the base-k digits of the integers, so it is not surprising that automatic sequences frequently arise from iteration. Suppose we iteratively replace the letters a and b in a word according to the morphism $a \to ab$ and $b \to ba$. Beginning with the word a, we obtain the sequence

$$\begin{aligned} a &\to ab \\ &\to abba \\ &\to abbabaab \\ &\to abbabaabbaababba \\ &\ \ \vdots \end{aligned}$$

which happens to consist of prefixes of the Thue–Morse sequence. In the limit, we obtain the Thue–Morse sequence itself, which is a fixed point of this morphism. Indeed, any morphism on a finite alphabet, where the image of each letter has length $k \geq 2$ and there is some letter a whose image begins with a, has an infinite fixed point. Cobham showed in 1972 that the letters of this fixed point form a k-automatic sequence.

Fixed points of morphisms are a central tool in combinatorics on words. A common question is whether a given pattern is avoidable in arbitrarily long words on a given alphabet. For instance, a *square* is a word of the form $w^2 = ww$, where w is a nonempty word. Are squares avoidable on a two-letter alphabet? Try to write down a long square-free word; it doesn't take long to determine whether this is possible. In 1912 Thue showed that cubes, i.e., words of the form w^3, are avoidable on a two-letter alphabet. His approach was to use properties of the morphism $a \to ab, b \to ba$ to conclude that the Thue–Morse sequence is cube-free.

In fact, Thue showed something stronger, namely, that the Thue–Morse sequence is overlap-free. An *overlap* is a word of the form wwc where w is a nonempty word whose first letter is c. Overlaps can be thought of as "$(2+\varepsilon)$-powers." Since overlaps are avoidable on a two-letter alphabet but squares are not, the exponent 2 is the *repetition threshold* for a two-letter alphabet.

Extensions of Thue's result have received much attention. In 1972 Dejean determined that the repetition threshold for a three-letter alphabet is $\frac{7}{4}$. A fractional power is a partial repetition; for example, *abbabbab* is the $\frac{8}{3}$-power $(abb)^{8/3}$. Dejean showed that it is not possible to avoid fractional $\frac{7}{4}$-powers on a three-letter alphabet, but it is possible to simultaneously avoid all $\frac{p}{q}$-powers with $\frac{p}{q} > \frac{7}{4}$. The morphism she used generates a 19-automatic sequence as opposed to Thue's 2-automatic sequence, but the broad idea of the proof is the same. For a general n-letter alphabet, Dejean's conjecture for the repetition threshold was finally confirmed through a number of additional papers by multiple authors. The last of these appeared only in 2011, nearly a century after Thue's results for a two-letter alphabet.

Automatic Sequences in Number Theory

Automatic sequences are also a useful tool in number theory, where they arise from an algebraic characterization of p-automatic sequences for prime p, which Christol discovered in 1979. Amazingly, p-automatic sequences correspond precisely to algebraic formal power series over finite fields $\mathbb{F}_q$ of characteristic p. That is, a sequence $s(n)_{n\geq 0}$ of elements in $\mathbb{F}_q$ is p-automatic if and only if $\sum_{n\geq 0} s(n)x^n$ is algebraic over $\mathbb{F}_q(x)$. For example, if we rename the letters in the alphabet for the Thue–Morse sequence, then the generating function $y = \sum_{n\geq 0} s(n)x^n$ of $s(n)_{n\geq 0} = 0, 1, 1, 0, 1, 0, 0, 1, \ldots$ satisfies

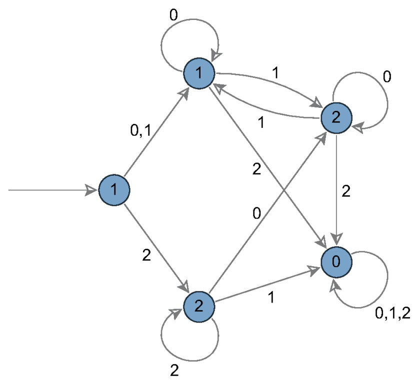
$$(1+x)^3y^2 + (1+x^2)y + x = 0$$

in $\mathbb{F}_2[\![x]\!]$.

An immediate application of this characterization is as follows. If $S(n)_{n\geq 0}$ is a sequence of integers such that $\sum_{n\geq 0} S(n)x^n$ is algebraic over $\mathbb{Q}(x)$, then projecting modulo p shows that

$$\sum_{n\geq 0} (S(n) \bmod p)x^n$$

is algebraic over $\mathbb{F}_p(x)$, and hence $(S(n) \bmod p)_{n\geq 0}$ is p-automatic. Many sequences that arise in enumeration settings have algebraic generating functions, so their behavior modulo primes can be assessed in this way. For example, the nth Catalan number $C(n) = \frac{1}{n+1}\binom{2n}{n}$ is the coefficient of x^n in one of the solutions of $xy^2 - y + 1 = 0$, so for any prime p we can produce an automaton for computing $C(n) \bmod p$. Here is an automaton that computes $C(n) \bmod 3$ when fed the base-3 digits of n:



Now consider the more general situation where we reduce an algebraic sequence modulo a prime power p^α. Since $\mathbb{Z}/(p^\alpha\mathbb{Z})$ is not a field for $\alpha \geq 2$, we can't use Christol's algebraic characterization to conclude that $(S(n) \bmod p^\alpha)_{n\geq 0}$ is p-automatic. However, Furstenberg showed that one can realize an algebraic sequence as the diagonal of a rational power series in two variables. The diagonal of a rational function lends itself to certain analyses, and it turns out to be good for computing an automaton for a sequence modulo p^α. Namely, there is an injection of the set of states of the automaton into the set of polynomials in $(\mathbb{Z}/(p^\alpha\mathbb{Z}))[x,y]$ with some bounded degree. Since this set is finite, the set of states is also finite and can be computed by polynomial arithmetic. The sequence of Catalan numbers forms the diagonal of

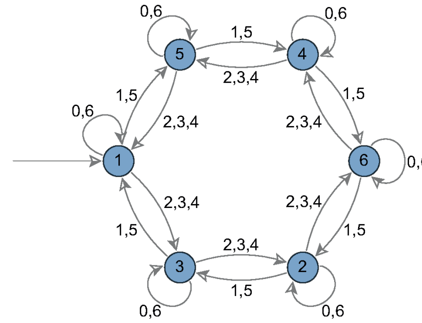
$$\frac{(y+1)\,(2xy^2+xy+x-1)}{xy^2+2xy+x-1}.$$

We can use this function to compute an automaton for $C(n) \bmod p^\alpha$ and obtain congruence information about the Catalan numbers. For example, $C(n) \not\equiv 3 \mod 4$ for all $n \geq 0$ simply because the automaton we compute does not output 3. Similar results for other sequences are completely routine to discover and prove [4].

Since this method works not just for algebraic sequences but more generally for diagonals of rational functions, it applies to many nonalgebraic combinatorial sequences as well as sequences that have arisen in number theoretic contexts. For example, the numbers $A(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$, which Apéry used to prove the irrationality of $\zeta(3)$, form the diagonal of

$$\frac{1}{(1-x_1-x_2)(1-x_3-x_4)-x_1x_2x_3x_4},$$

so $(A(n) \bmod p^\alpha)_{n\geq 0}$ is p-automatic. For $\alpha = 1$ this also follows from a result of Gessel, who proved that, if we write $n = n_l \cdots n_1 n_0$ in base p, then $A(n) \equiv \prod_{i=0}^{l} A(n_i) \mod p$. For $p^\alpha = 7$ we get the following particularly symmetric automaton which computes $A(n) \bmod 7$. The loops labeled $0, 6$ reflect that $A(0) \equiv A(6) \equiv 1 \mod 7$.



If $S(n)_{n\geq 0}$ is the diagonal of a rational power series, then $S(n)_{n\geq 0}$ is holonomic, meaning that it satisfies a linear recurrence with coefficients that are polynomials in n. Not every holonomic sequence is the diagonal of a rational power series; for example, $n!_{n\geq 0}$ grows too quickly. However, a conjecture of Christol [2] implies that every holonomic sequence of integers that grows at most exponentially is the diagonal of a rational function. If this conjecture is true, then essentially every sequence that arises in combinatorics is p-automatic when reduced modulo p^α.

Further Reading

[1] Jean-Paul Allouche and Jeffrey Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[2] Gilles Christol, Globally bounded solutions of differential equations, in *Analytic Number Theory (Tokyo, 1988)*, Lecture Notes in Mathematics, 1434, Springer-Berlin, 1990, pp. 45–64.

[3] James D. Currie, Pattern avoidance: themes and variations, *Theoretical Computer Science* **339** (2005), 7–18.

[4] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *Journal de Théorie des Nombres de Bordeaux*, to appear. `http://arxiv.org/abs/1310.8635` (2014).