Automata and finite order elements in the Nottingham group.

Jakub Byszewski

joint work with Gunther Cornelissen and Djurre Tijsma

JAGIELLONIAN UNIVERSITY
IN KRAKÓW

21 June 2021

The Nottingham group

Let p be a prime number. The Nottingham group $\mathcal{N}(\mathbf{F}_p)$ consists of power series of the form

$$t + a_2 t^2 + a_3 t^3 + \cdots$$

with coefficients from $\mathbf{F}_p$ with substitution as group multiplication.

It can be described as the pro-p-Sylow subgroup of the group of ring automorphisms $\mathrm{Aut}(\mathbf{F}_p[\![t]\!])$ of the formal power series ring $\mathbf{F}_p[\![t]\!]$, with composition as multiplication.

Camina and Jennings proved that every metrisable pro-p group embeds into $\mathcal{N}(\mathbf{F}_p)$; in particular, every finite p-group embeds into $\mathcal{N}(\mathbf{F}_p)$.

Aim

The group $\mathcal{N}(\mathbf{F}_p)$ has many elements of finite order (the order is necessarily a power of p). Describe them explicitly!

Klopsch theorem

Theorem (Klopsch, 1990)

Every element of order p in $\mathcal{N}(\mathbf{F}_p)$ is conjugate to a unique element of the form

$$\sigma(t) = \frac{t}{\sqrt[m]{1 + at^m}}$$

with $a \in \mathbf{F}_p^*$ and $m \in \mathbf{N}$ coprime to p.

In fact,

$$\sigma^{\circ k}(t) = \frac{t}{\sqrt[m]{1 + kat^m}}.$$

What about series of order p^2, p^3, etc.?

Examples

Previously, the only known examples of explicit power series of order $\geqslant p^2$ were of order 4 for $p = 2$.

- Example of Chinburg and Symonds:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k\geqslant 0} \sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k + 2\ell} = t + t^2 + O(t^6).$$

- Its compositional inverse, computed by Scherr and Zieve:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k\geqslant 0} \left(t^{3\cdot 2^k - 2} + t^{4\cdot 2^k - 2} \right) = t + t^2 + t^4 + O(t^6).$$

- Example of Jean:

$$\sigma_{\mathrm{J}}(t) := t + t^2 \frac{1 + t^5}{1 + t^8} + \sum_{k\geqslant 2} t^{2^k} \frac{t^{2^{k+1}} + t}{t^{2^{k+2}} + 1} = t + t^2 + t^5 + O(t^6).$$

Break sequence

Definition

The depth of $\sigma = \sigma(t) \in \mathcal{N}(\mathbf{F}_p)$ is

$$d(\sigma) = \operatorname{ord}_t(\sigma(t) - t) - 1$$

(and $d(t) = \infty$), so if $\sigma(t) = t + a_k t^k + O(t^{k+1})$ with $a_k \neq 0$, then $d(\sigma) = k - 1$.

The (lower) break sequence of $\sigma \in \mathcal{N}(\mathbf{F}_p)$ with finite order p^n is defined as

$$\mathfrak{b}_\sigma = (b_i)_{i=0}^{n-1} = (d(\sigma^{\circ p^i}))_{i=0}^{n-1}.$$

The break sequence is an invariant of conjugation.

The power series $t/\sqrt[m]{1 + at^m}$ has break sequence (m) (for $a \in \mathbf{F}_p^*$).

The examples of Chinburg–Symonds, Scherr–Zieve and Jean all have 'minimal' break sequence $(1, 3)$.

Classifying torsion elements

One can use local class field theory to describe all torsion elements. There are only finitely many elements with given order and break sequence. However, the classification is not quite explicit.

Theorem (Lubin, 2011)

Write $U_1 = 1 + t\,\mathbf{F}_p[\![t]\!]$. There is a bijection between conjugacy classes of order-p^n elements in $\mathcal{N}(\mathbf{F}_p)$ and strict equivalence classes of continuous surjective characters $\eta\colon U_1 \to \mathbf{Z}/p^n\mathbf{Z}$.
We say that η and η' are strictly equivalent if there exists $u \in \mathcal{N}(\mathbf{F}_p)$ with

$$\eta(u(z)/z) = 0 \quad \text{and} \quad \eta'(x) = \eta(x \circ u) \quad \text{for all} \quad x \in U_1.$$

Via this bijection, one may also read off the break sequence of an element from the corresponding character. However, there is no known formula for the number of conjugacy classes of elements of given order and break sequence, and while the coefficients of the corresponding power series can be computed recursively, this usually does not lead to explicit formulæ.

By a rather deep result of Harbater, every embedding of a finite p-group in $\mathcal{N}(\mathbf{F}_p)$ comes from a G-covering $\pi\colon X \to \mathbf{P}^1$, where X is a smooth curve with an action of G, and the map π is totally ramified over ∞ and unramified elsewhere.

Corollary

Every finite order automorphism in $\mathcal{N}(\mathbf{F}_p)$ is conjugate to a power series that is algebraic over $\mathbf{F}_p(t)$.

Every finite group of automorphism in $\mathcal{N}(\mathbf{F}_p)$ is conjugate to a group whose elements are power series that are algebraic over $\mathbf{F}_p(t)$.

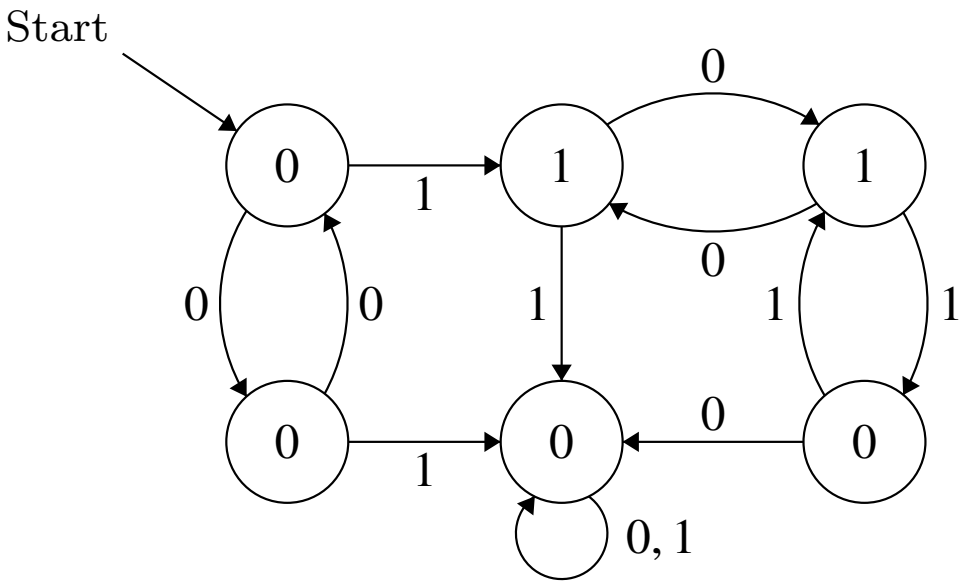
Hence, by Christol's theorem every conjugacy class contains a series whose coefficients are produced by an automaton!

Example:

Consider Klopsch's series

$$\sigma_{\mathrm{K},3} := t/\sqrt[3]{1+t^3} = \sum_{k\geqslant 0} a_{3k+1}t^{3k+1} = t + t^4 + t^{13} + \cdots \in \mathcal{N}(\mathbf{F}_2)$$

The coefficients can be described explicitly: $a_k = 1$ if and only if the base-4 expansion of $k-1$ contains only the digits 0 or 3, or by an automaton:



Christol's theorem

Theorem (Christol, 1979)

A series $\sum_{n\geqslant 0} a_n t^n \in \mathbf{F}_p[\![t]\!]$ is algebraic if and only if the sequence (a_n) is p-automatic.

Klopsch's series satisfies the equation $(1+t^3)X^3 + t = 0$.

Thue–Morse's series satisfies the equation $t + (1+t)^2 X + (1+t)^3 X^2 = 0$.

Idea of the proof: a sequence (a_n) is p-automatic iff its p-kernel

$$N((a_n)) = \{(a_{p^i n+j})_n \mid i \geqslant 0, 0 \leqslant j < p^i\}$$

is finite. This corresponds to Cartier operators C_r on power series:

$$C_r\Big(\sum a_i t^i\Big) = \sum a_{pi+r} t^i.$$

The essence of the proof is to show that if f is algebraic, then f lies in a finitely dimensional $\mathbf{F}_p$-vector space that is invariant under the action of the Cartier operators.

Constructing finite order automorphism

Strategy

1. Write down explicit equations for a cyclic totally ramified p^n-extension of the field $\mathbf{F}_p(\!(z)\!)$ which is defined over $\mathbf{F}_p(z)$. This can be done using either Witt vectors or torsion of the Carlitz module.
2. Choose a uniformiser t as an algebraic function of the chosen field generators.
3. Compute the action of a generator σ of the Galois group on the uniformiser t and express it as an algebraic equation between t and $\sigma(t)$.
4. Use (a proof of) Christol's theorem to find an automaton producing $\sigma(t)$.

First example

We want to construct a totally ramified cyclic degree-4 extension $K/\mathbf{F}_2((z))$. We can use Witt vectors to produce the extension $K = \mathbf{F}_2((z))(x, y)$ with

$$\begin{cases} x^2 + x = z^{-1}; \\ y^2 + y = xz^{-1} = x^3 + x^2, \end{cases}$$

An example of a uniformiser t for K is given by $t = (y + 1)/(y + x^2)$. A generator σ of the Galois group is determined by the equations

$$\begin{cases} \sigma(x) = x + 1; \\ \sigma(y) = y + x + 1, \end{cases}$$

We compute

$$\sigma(t) = \frac{y + x}{y + x^2 + x}.$$

To find an algebraic equation for σ over $\mathbf{F}_2(t)$, we need to eliminate x and y:

$$\begin{cases} y^2 + y = x^3 + x^2 & \text{[equation of extension]}; \\ (y + x^2)t = y + 1 & \text{[definition of uniformiser]}; \\ (y + x^2 + x)\sigma(t) = y + x & \text{[action of } \sigma \text{ on uniformiser]}, \end{cases}$$

from which we get that σ satisfies the equation

$$F(t, X) = (t + 1)^3X^3 + (t^3 + t)X^2 + (t^3 + t + 1)X + t^3 + t = 0. \tag{1}$$

This equation has a unique solution of the form $t + O(t^2)$.

Constructing the automaton

To construct the automaton, one needs to explicitly construct a vector space V, Cartier operators $C_r : V \to V$, an element $v \in V$, and the output map $\tau : V \to \mathbf{F}_p$ that emulates the behaviour of the Cartier operators on the space spanned by $f \in \mathbf{F}_p[\![t]\!]$ and its images via Cartier operators. There are three main choices:

1. Ore form. Convert the algebraic equation to the form

$$a_n f^{p^n} + a_{n-1} f^{p^{n-1}} + \cdots + a_0 = 0, \qquad a_i \in \mathbf{F}_p[\![t]\!].$$

   then take

$$V = \bigoplus_{i=0}^{n-1} \mathbf{F}_p[t]_{\leqslant N} X^{p^i} \quad \text{for sufficiently large } N.$$

2. Differential forms. Let X be the curve defined by the (irreducible factor of the) equation. Take

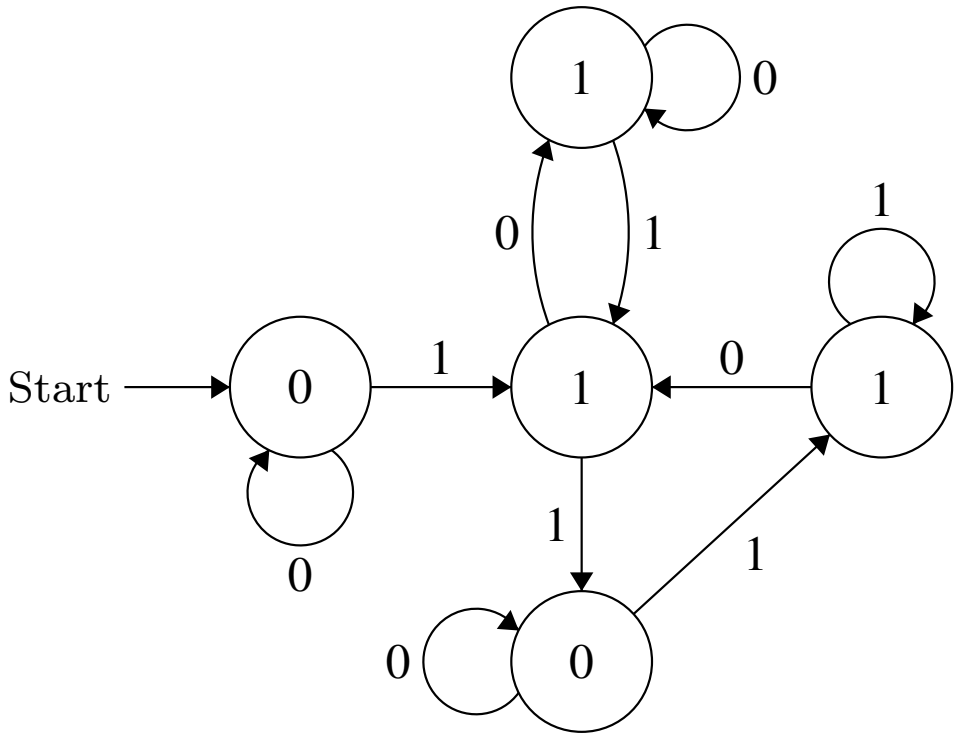
$$V = \Omega_X(D) \quad \text{for sufficiently large divisor } D.$$

3. Diagonals of rational functions. Use Furstenberg's theorem to write f as the diagonal of a two-variable rational function $P/Q \in \mathbf{F}_p(X, Y)$. Take

$$V = \{\frac{P'}{Q} \mid P' \in \mathbf{F}_p[X, Y], \deg P' \leqslant N\} \quad \text{for sufficiently large } N.$$

First example

For our element of order 4, this method produces the series $\sigma_{\min}$ generated by the following automaton:



Ragnar Groot Koerkamp computed that this is the smallest automaton producing an element of order 4.

Repertoire of examples

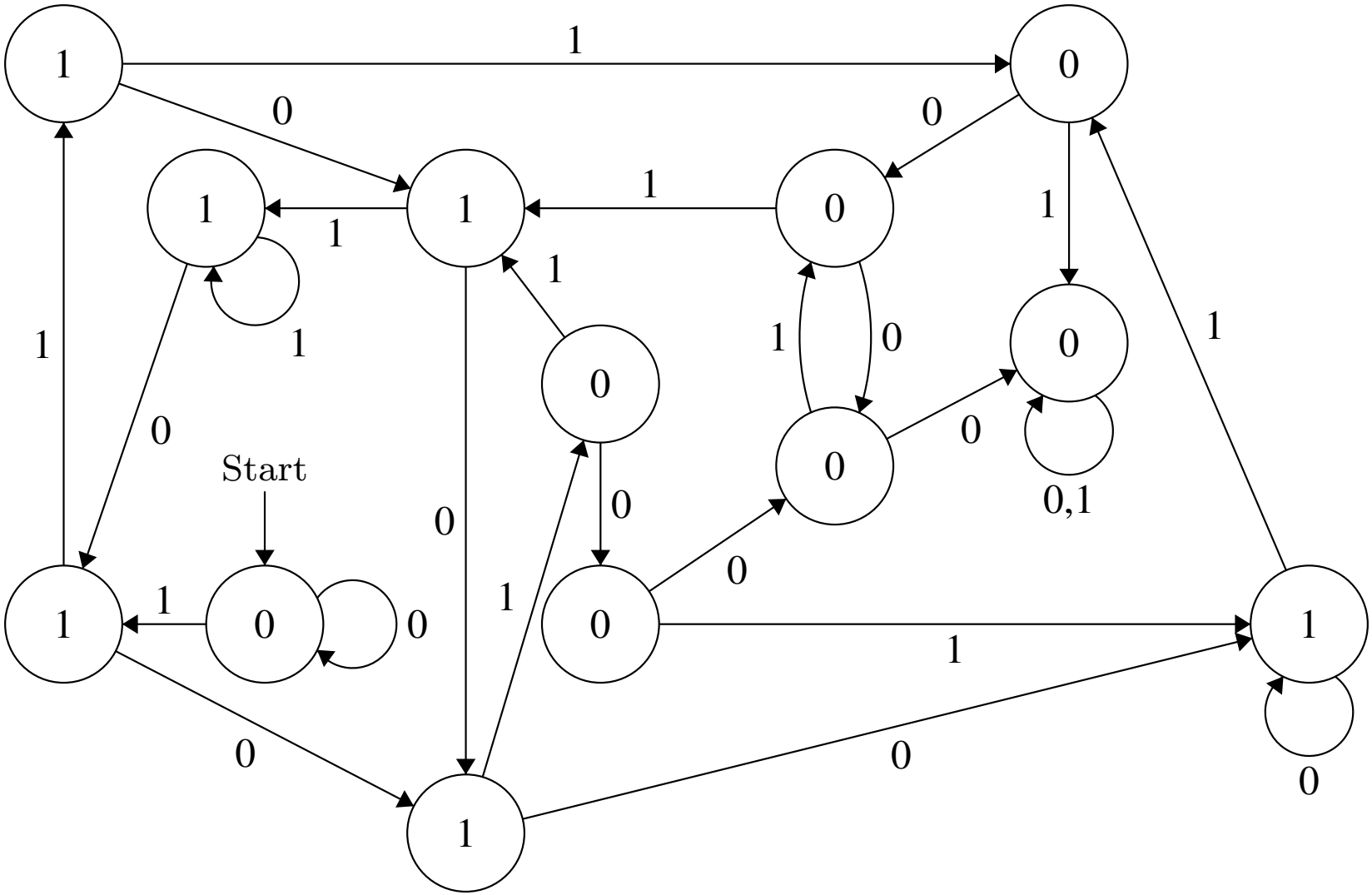
We construct automata producing series representing all the conjugacy classes of the following series:

- of order 4 and break sequence $(1,3)$. There are two conjugacy classes represented by $\sigma_{\min}$ and $\sigma_{\min}^{\circ 3}$. The Chinburg–Symonds series is conjugate to $\sigma_{\min}$, and Jean series is conjugate to $\sigma_{\min}^{\circ 3}$.
- of order 4 and break sequence $(1,5)$. There is one conjugacy class. Our automaton has 13 states.
- of order 4 and break sequence $(1,9)$. There is one conjugacy class. Our automaton has 110 states.
- of order 8 and 'minimal' break sequence $(1,3,11)$. There are four conjugacy classes represented by $\sigma_{8,1}, \sigma_{8,1}^{\circ 3}, \sigma_{8,2}, \sigma_{8,2}^{\circ 3}$. The automata producing $\sigma_{8,1}$ and $\sigma_{8,2}$ have 320 and 926 states.

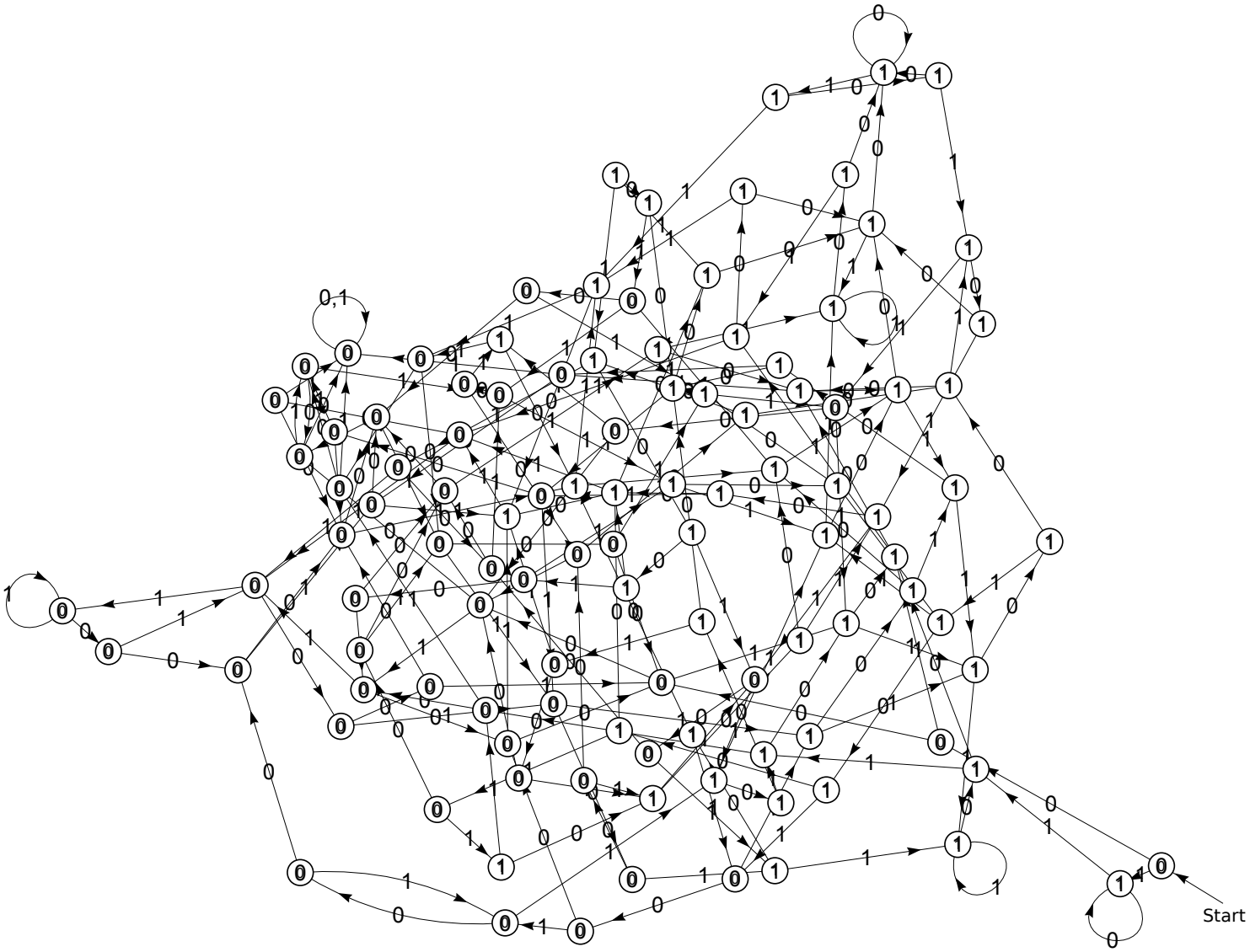
We also have automata generating:

- a series of order 9 and break sequence $(1,7)$. Our automaton has 3634 states.
- an embedding of the Klein four-group, given by automata with 14, 18 and 25 states.
- an embedding of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ with generators produced by automata with 128 states.

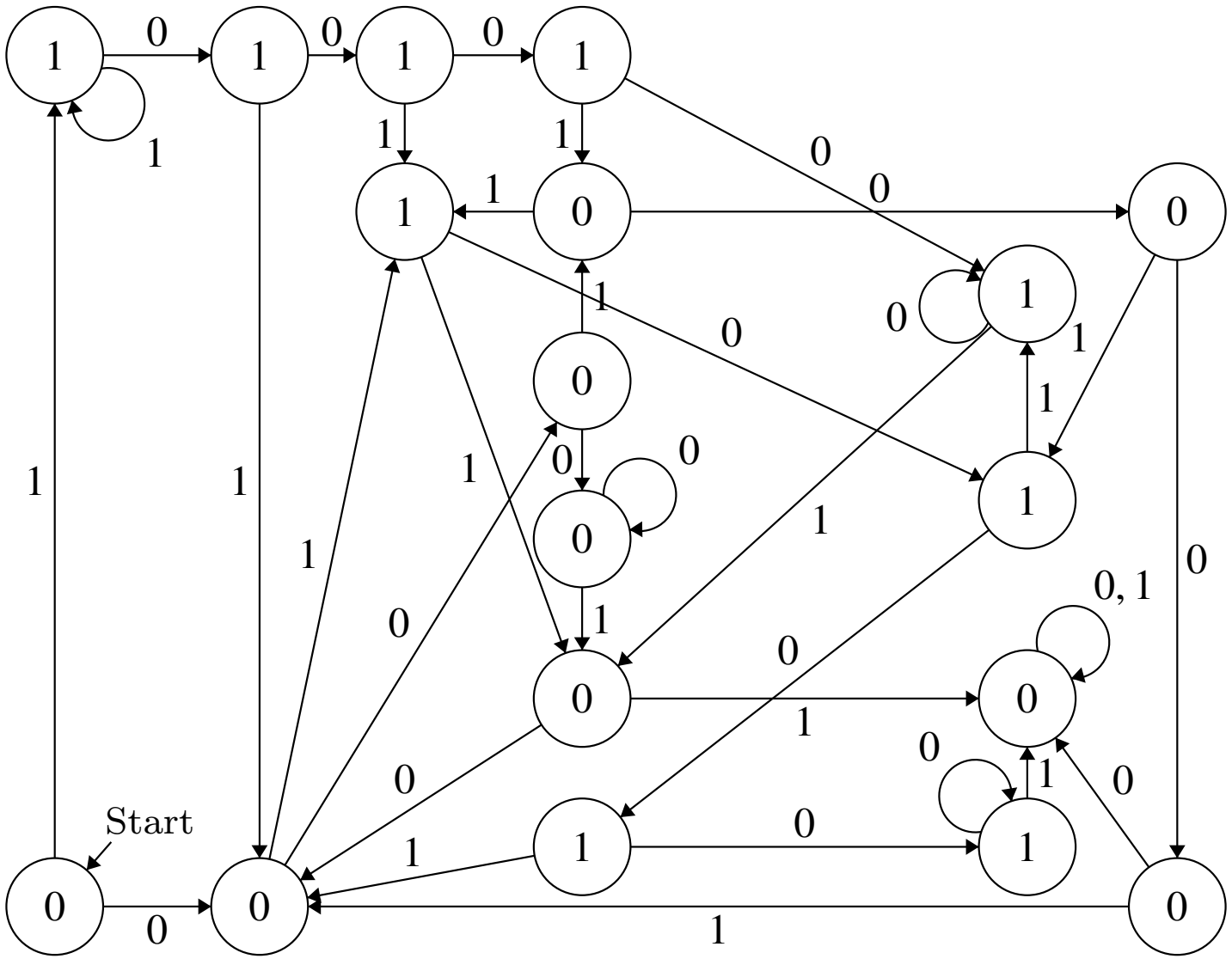
An automaton generating a power series of order 4 and break sequence $(1, 5)$



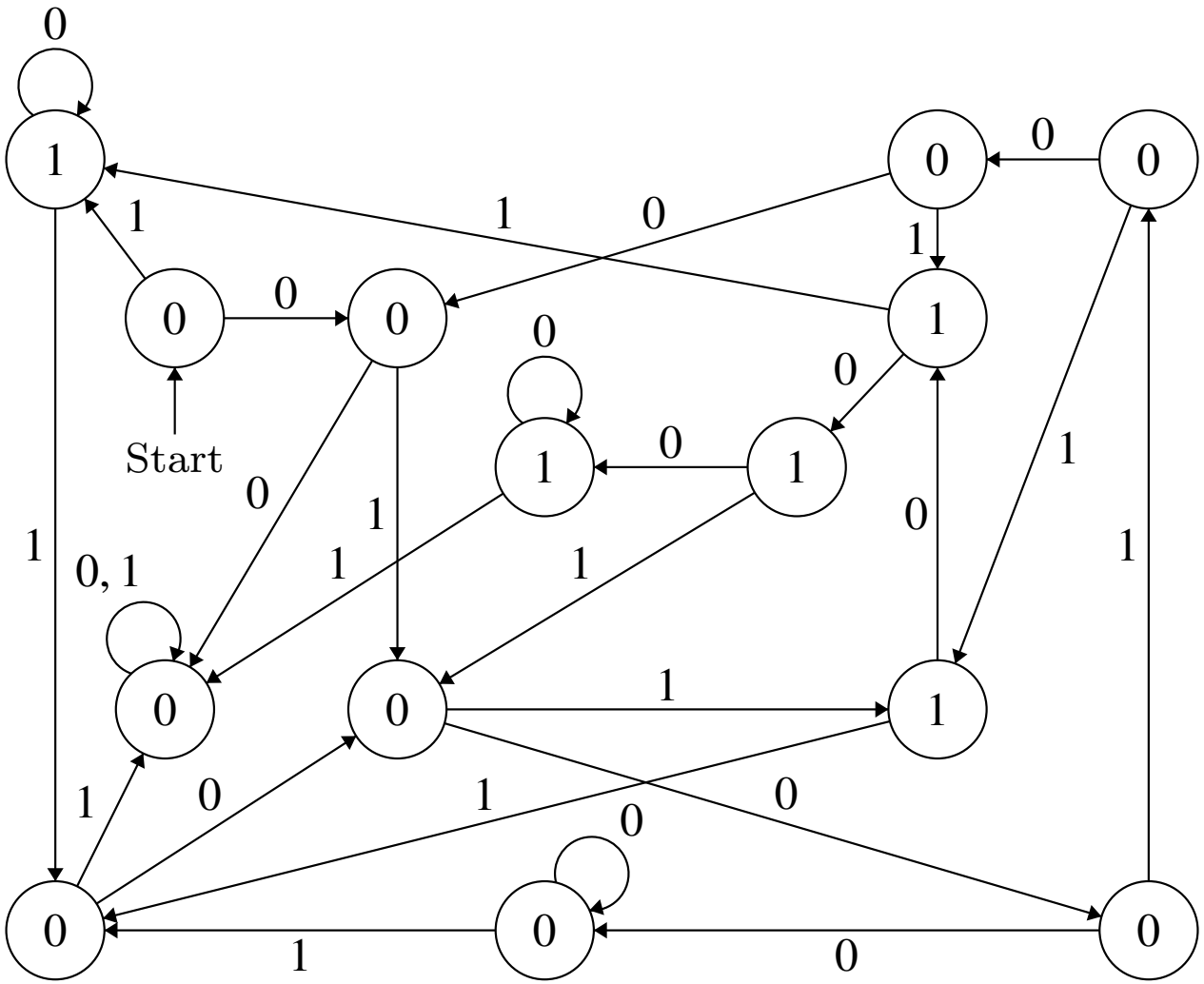
An automaton generating a power series of order 4 and break sequence $(1, 9)$



An automaton generating one of the generators of the Klein four-group



An automaton generating another of the generators of the Klein four-group



And so what?

Ok, so now that you have all these automata, what can you use them for? What kind of new questions can you ask?

Sparseness

For a power series $\sigma = \sum a_k t^k \in \mathbf{F}_p[\![t]\!]$, the support of σ, i.e. the set of integers k for which $a_k \neq 0$.

Theorem (Cobham, 1972)

Let $\sigma \in \mathbf{F}_p[\![t]\!]$ be an algebraic power series. Then exactly one of the following conditions holds:

1. either $\#(E(\sigma) \cap \{0, 1, \ldots, N\}) \geqslant N^\alpha$ for some real $\alpha > 0$ and large N;
2. or $\#(E(\sigma) \cap \{0, 1, \ldots, N\}) \leqslant (\log N)^r$ for some r.

In the latter case, the series is called sparse, and the smallest such r is an integer called the rank of sparseness.
Define a simple sparse set of rank at most r to be a set of integers whose base-p expansion is of the form $v_r w_r^{\ell_r} \cdots v_1 w_1^{\ell_1} v_0$ with $\ell_i \in \mathbf{Z}_{\geqslant 0}$ for some fixed words $v_0, \ldots, v_r, w_1, \ldots, w_r$.

Theorem (Szilard, Yu, Zhang and Shallit, 1992)

An algebraic series σ is sparse of rank at most r precisely if $E(\sigma)$ is a finite union of pairwise disjoint simple sparse sets of rank at most r.

Examples

- The series of Scherr–Zieve is sparse:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k\geqslant 0} \left(t^{3\cdot 2^k - 2} + t^{4\cdot 2^k - 2} \right) = t + t^2 + t^4 + O(t^6).$$

- The series of Chinburg–Symonds is a product of a sparse series and a rational function:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k\geqslant 0} \sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k + 2\ell} = t + t^2 + O(t^6).$$

- The series of Jean is a product of a sparse series and a rational function after the substitution $t \mapsto t/(t+1)$:

$$\sigma_{\mathrm{J}}(t) := t + t^2 \frac{1+t^5}{1+t^8} + \sum_{k\geqslant 2} t^{2^k} \frac{t^{2^{k+1}} + t}{t^{2^{k+2}} + 1} = t + t^2 + t^5 + O(t^6).$$

- The series $\sigma_{\min}$ is not of this type.

Theorem of Albayrak–Bell

Theorem (Albayrak–Bell, special case)

Let $\sigma \in \mathbf{F}_p[\![t]\!]$ denote a power series that is algebraic over $\mathbf{F}_p(t)$. Consider the field

$$\mathcal{F} = \bigcup_{\substack{\ell \geqslant 1, \\ p \nmid \ell}} \overline{\mathbf{F}}_2(t^{1/\ell}),$$

where $\overline{\mathbf{F}}_p$ is an algebraic closure of $\mathbf{F}_p$. If σ is sparse, then the following conditions hold:

1. σ is integral over $\overline{\mathbf{F}}_p[t, t^{-1}]$;
2. the extension $\overline{\mathbf{F}}_p(t)(\sigma)/\overline{\mathbf{F}}_p(t)$ is unramified outside of $0, \infty$;
3. the splitting field of σ over $\mathcal{F}$ has degree a power of two.

Theorem

Let m be an integer of the form $m = 2^\mu \pm 1$ for $\mu \geqslant 1$. Then any power series of order 2 and break sequence (m) is conjugate to a sparse power series. More precisely, we have the following:

1. Any power series of order 2 and break sequence (1) is conjugate to the sparse power series

$$\sigma_{S,1} = t + \sum_{k \geqslant 2} \left(t^{2^k - 2} + t^{2^k - 1} \right). \tag{2}$$

2. If $m = 2^\mu - 1 > 1$, then any power series of order 2 and break sequence (m) is conjugate to the sparse power series

$$\sigma_{S,m} = t + \sum_{k \geqslant 1} t^{\frac{m+1}{m-1}\left(m \cdot \left(\frac{m+1}{2}\right)^{k-1} - 1\right)}. \tag{3}$$

   The set of exponents occurring in σ consists of the integers whose base-2 representation is either 1 or $10^{\mu-1}(10^{\mu-2})^\ell 0$ for some $\ell \in \mathbf{Z}_{\geqslant 0}$.

Theorem (continued)

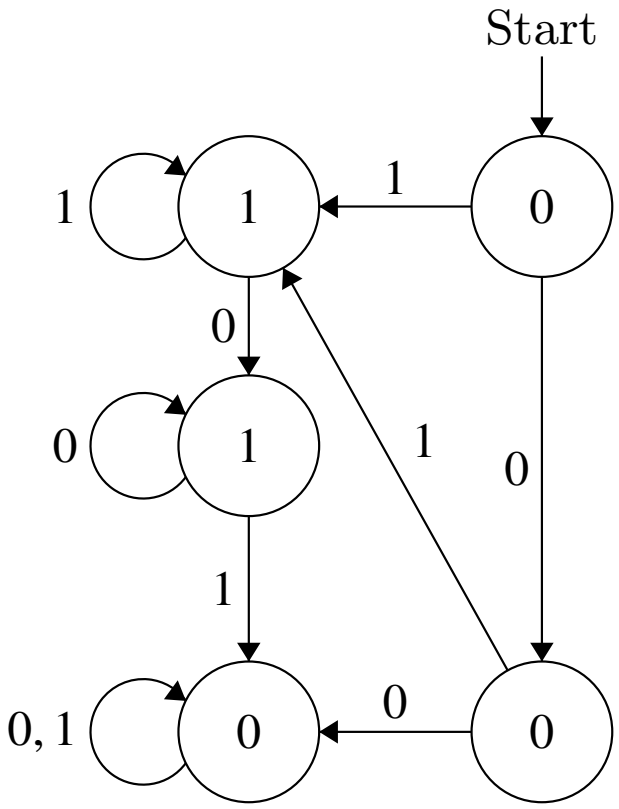
3 If $m = 2^\mu + 1$, then any power series of order 2 and break sequence (m) is conjugate to the sparse power series

$$\sigma_{S,m} = \sum_{\substack{\emptyset \neq J \subseteq \{0,\dots,\mu-1\} \\ k\colon J \to \mathbf{Z}_{\geqslant 0}}} t^{\left(\sum_{j\in J} 2^j (m-1)^{k(j)}\right) m - m + 1}. \tag{4}$$

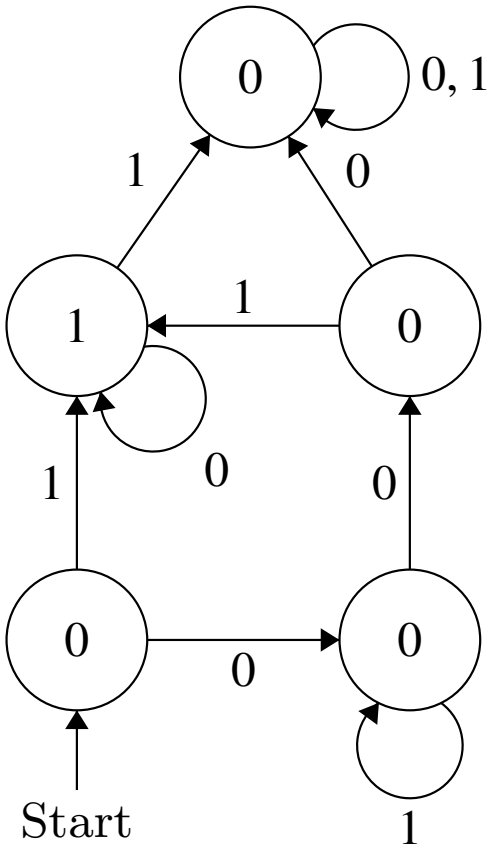
The support of $\sigma_{S,m}$ consists precisely of the integers $m(\ell - 1) + 1$ with $\ell \geqslant 1$ an integer whose base-2 expansion contains at most μ occurrences of the digit 1 and all these occurrences are at distinct positions modulo μ.

We also have sparse representatives of both conjugacy classes of minimally ramified order-4 elements (one of them is given by Scherr–Zieve).

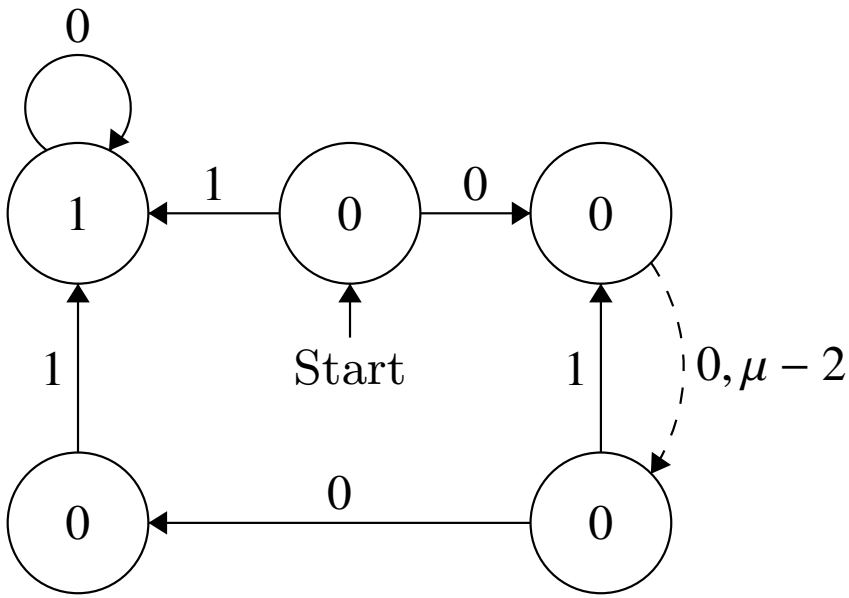
The automaton generating a sparse power series of order 2 and depth 1



An automaton generating a sparse power series of order 2 and depth 3



An automaton generating a sparse power series of order 2 and depth $2^\mu - 1$, $\mu \geqslant 3$



The dashed arrow replaces a path consisting of $\mu - 3$ vertices and $\mu - 2$ edges, all with label zero. The remaining missing edges all connect to a unique vertex with label 0, which has been omitted in order to simplify the graphical representation of the automaton.

Open questions

- Give an automaton-theoretic characterisation of series that are sparse up to multiplication with a rational function.
- Are the 'p-automata of finite order' somehow special from a combinatorial or automaton-theoretic point of view? Is there a characterisation in terms of the associated substitutions?
- How to test whether two algebraic power series are conjugate in $\mathcal{N}(\mathbf{F}_p)$?
- Is there a sparse series of order 2 with break sequence (11)? This is equivalent to asking whether Klopsch's series $t/\sqrt[11]{1+t^{11}} \in \mathcal{N}(\mathbf{F}_2)$ is conjugate to a sparse series. More generally, is every element of finite order in $\mathcal{N}(\mathbf{F}_2)$ sparse up to conjugation?
- Devise an algorithm that finds all automata on at most N states that represent series of finite order. For any given finite order this is easy, so what one needs is a bound on the order of a series in terms of the number of states of an automaton that generates it.