Automata and finite order elements in the Nottingham group.

Jakub Byszewski

joint work with Gunther Cornelissen, Djurre Tijsma, and Mieke Wessel

JAGIELLONIAN UNIVERSITY
IN KRAKÓW

16 June 2026

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 composition/substitution as group multiplication.

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 composition/substitution as group multiplication.

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 composition/substitution as group multiplication.

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!

The Nottingham group

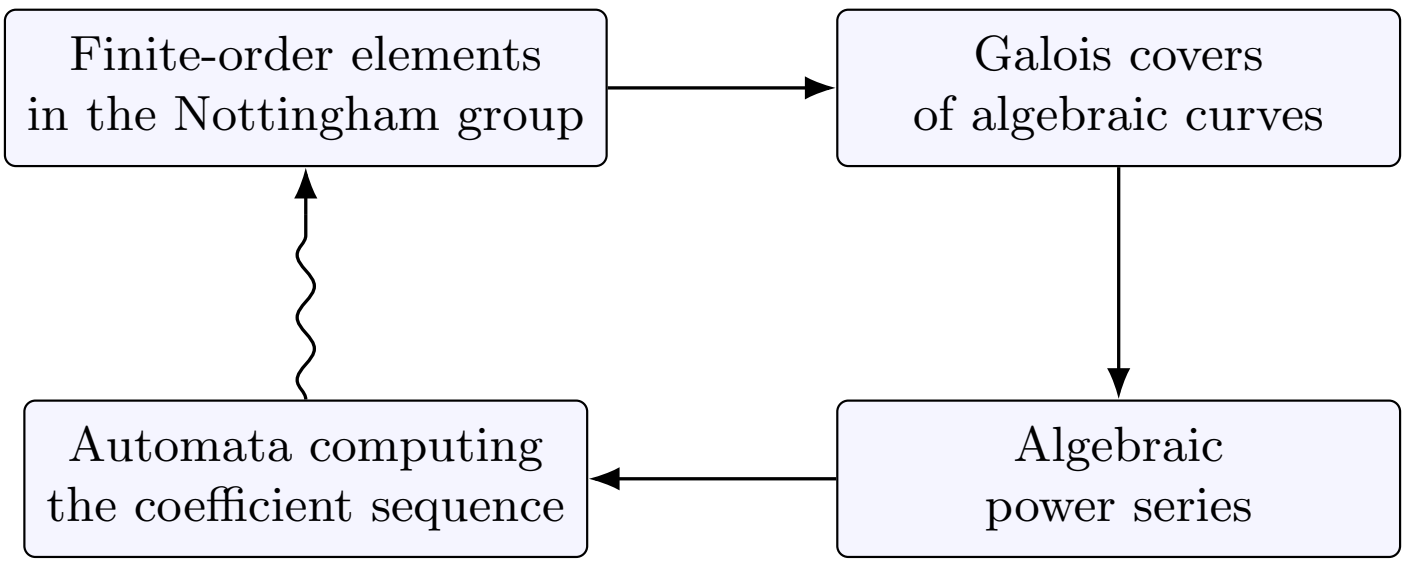
Let p be a prime number. The Nottingham group $\mathcal{N}(\mathbf{F}_p)$ consists of power series of the form

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

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

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

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

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

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

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

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

In fact,

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

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

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

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.?

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

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

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.?

In general, there are finitely many conjugacy classes of power series of order p^n with a given break sequence — a discrete invariant recording the first nontrivial term of σ, $\sigma^{\circ p}$, $\sigma^{\circ p^2}, \ldots, \sigma^{\circ p^{n-1}}$ (Lubin, 2011).

Examples

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

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:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k \geqslant 0} \sum_{\ell=0}^{2^k - 1} t^{6 \cdot 2^k + 2\ell} = t + t^2 + t^6 + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + \cdots .$$

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:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k\geqslant 0}\sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k+2\ell} = t + t^2 + t^6 + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + \cdots .$$

- Its compositional inverse, computed by Scherr and Zieve:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k\geqslant 0}\left(t^{3\cdot 2^k-2} + t^{4\cdot 2^k-2}\right) = t + t^2 + t^4 + t^6 + t^{10} + t^{14} + t^{22} + t^{30} + \cdots$$

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:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k\geqslant 0}\sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k+2\ell} = t + t^2 + t^6 + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + \cdots .$$

- Its compositional inverse, computed by Scherr and Zieve:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k\geqslant 0}\left(t^{3\cdot 2^k-2} + t^{4\cdot 2^k-2}\right) = t + t^2 + t^4 + t^6 + t^{10} + t^{14} + t^{22} + t^{30} + \cdots$$

- Example of Jean:

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

Christol's theorem and HKG covers

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.

Christol's theorem and HKG covers

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.

Can finite-order elements be represented by algebraic power series?

Christol's theorem and HKG covers

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.

Can finite-order elements be represented by algebraic power series?

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.

Christol's theorem and HKG covers

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.

Can finite-order elements be represented by algebraic power series?

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

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

Christol's theorem and HKG covers

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.

Can finite-order elements be represented by algebraic power series?

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

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

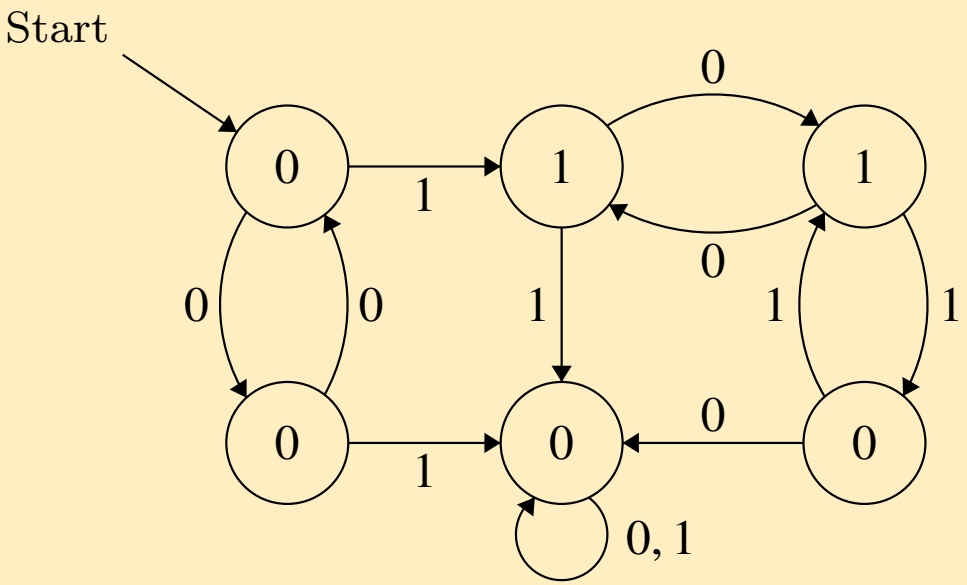
Hence, by Christol's theorem every conjugacy class contains a series whose coefficients are produced by an automaton!

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 are given by the automaton:



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 $t + Q(t^2)$.

First example

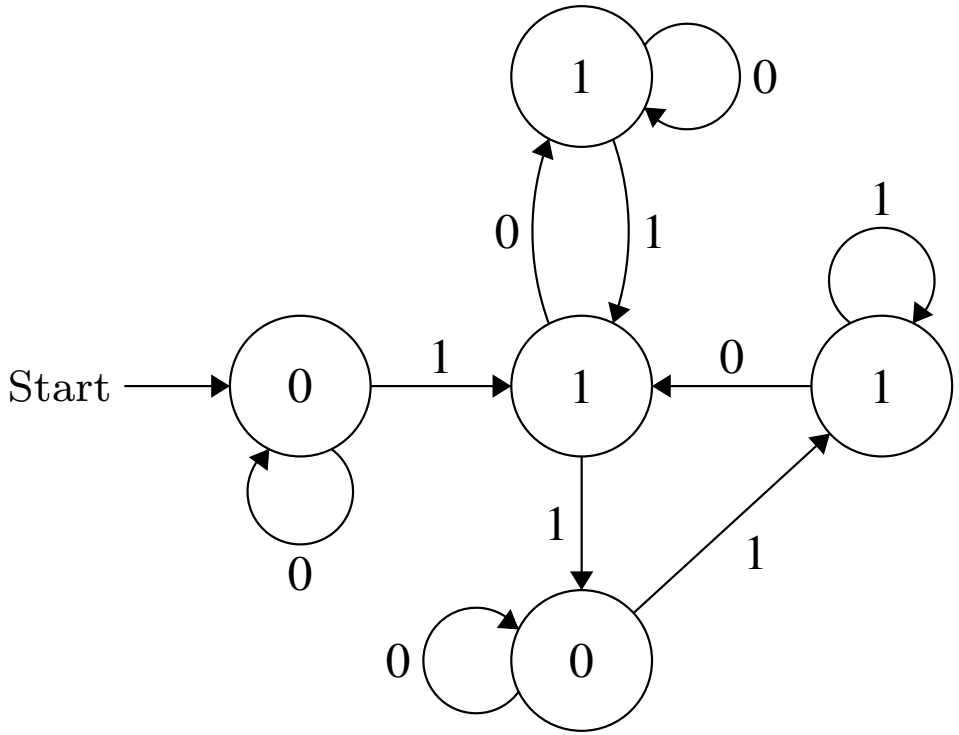
Given the equation, we apply Christol's theorem to produce an automaton.

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

First example

Given the equation, we apply Christol's theorem to produce an automaton.

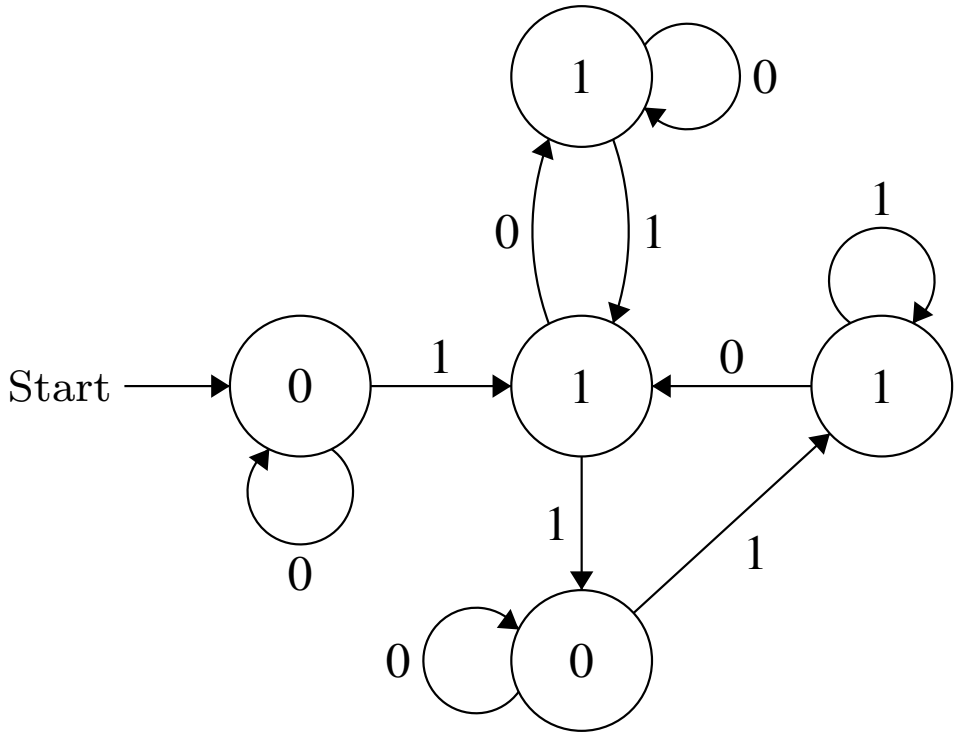
For our element of order 4, this method produces the series $\sigma_{\min}$ generated by the following automaton:



First example

Given the equation, we apply Christol's theorem to produce an automaton.

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:

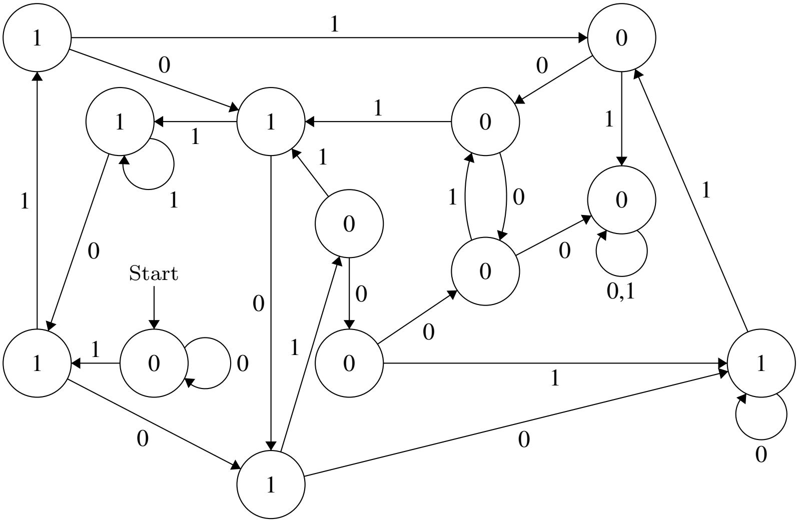
- order 4, break sequence $(1, 3)$. Our automaton has 5 states.
- order 4, break sequence $(1, 5)$. Our automaton has 13 states.
- order 4, break sequence $(1, 9)$. Our automaton has 110 states.
- order 8, break sequence $(1, 3, 11)$. Our automaton has 320 states.

We also have automata generating:

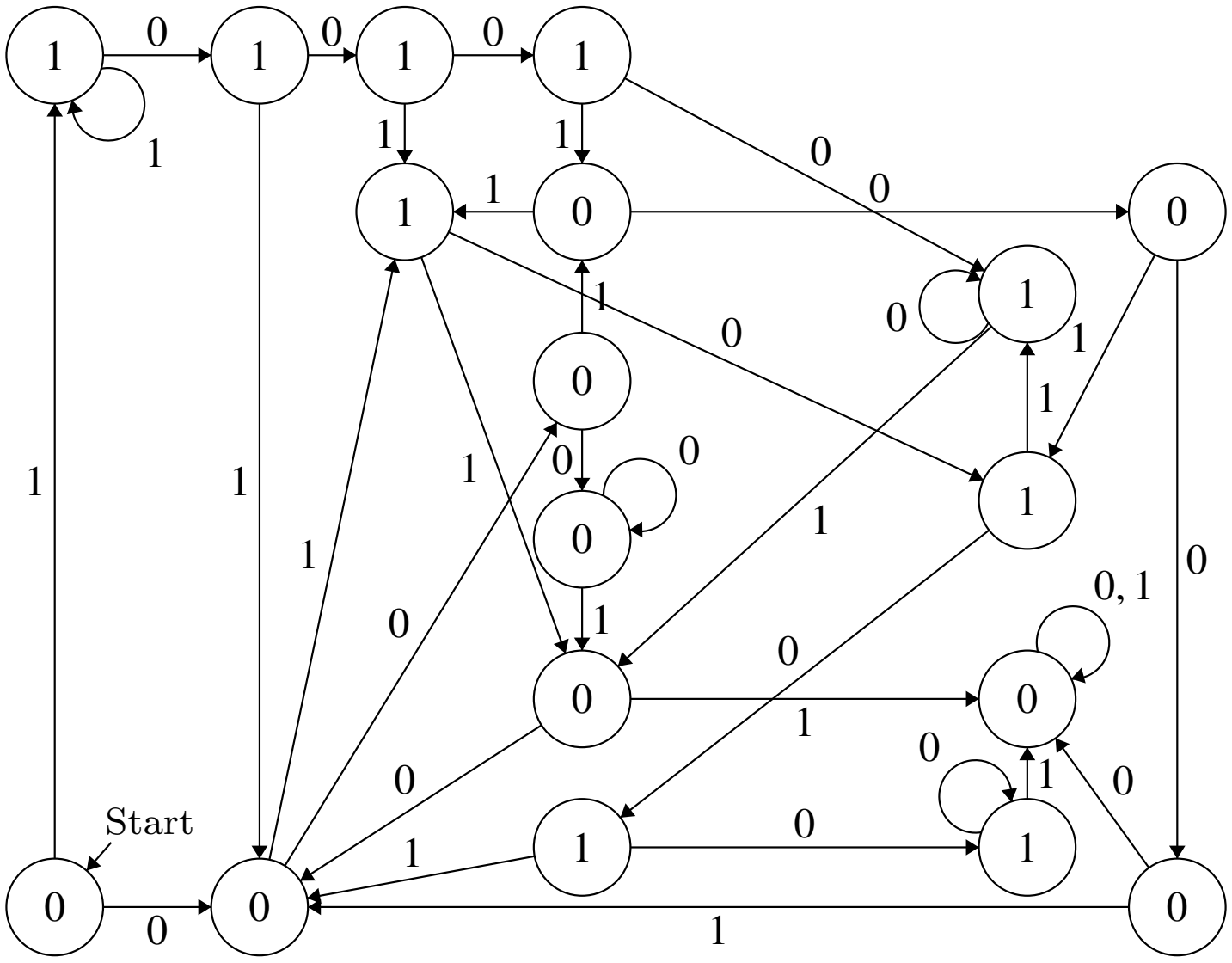
- order 9, break sequence $(1, 7)$. Our automaton has 3634 states.
- an embedding of the Klein four-group, given by automata with 14, 18 and 25 states.
- an embedding of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ with generators produced by automata with 128 states.

In 2025 Keating constructed automata giving an embeddings of Q_8 and D_4 into the Nottingham group over $\mathbf{F}_4$.

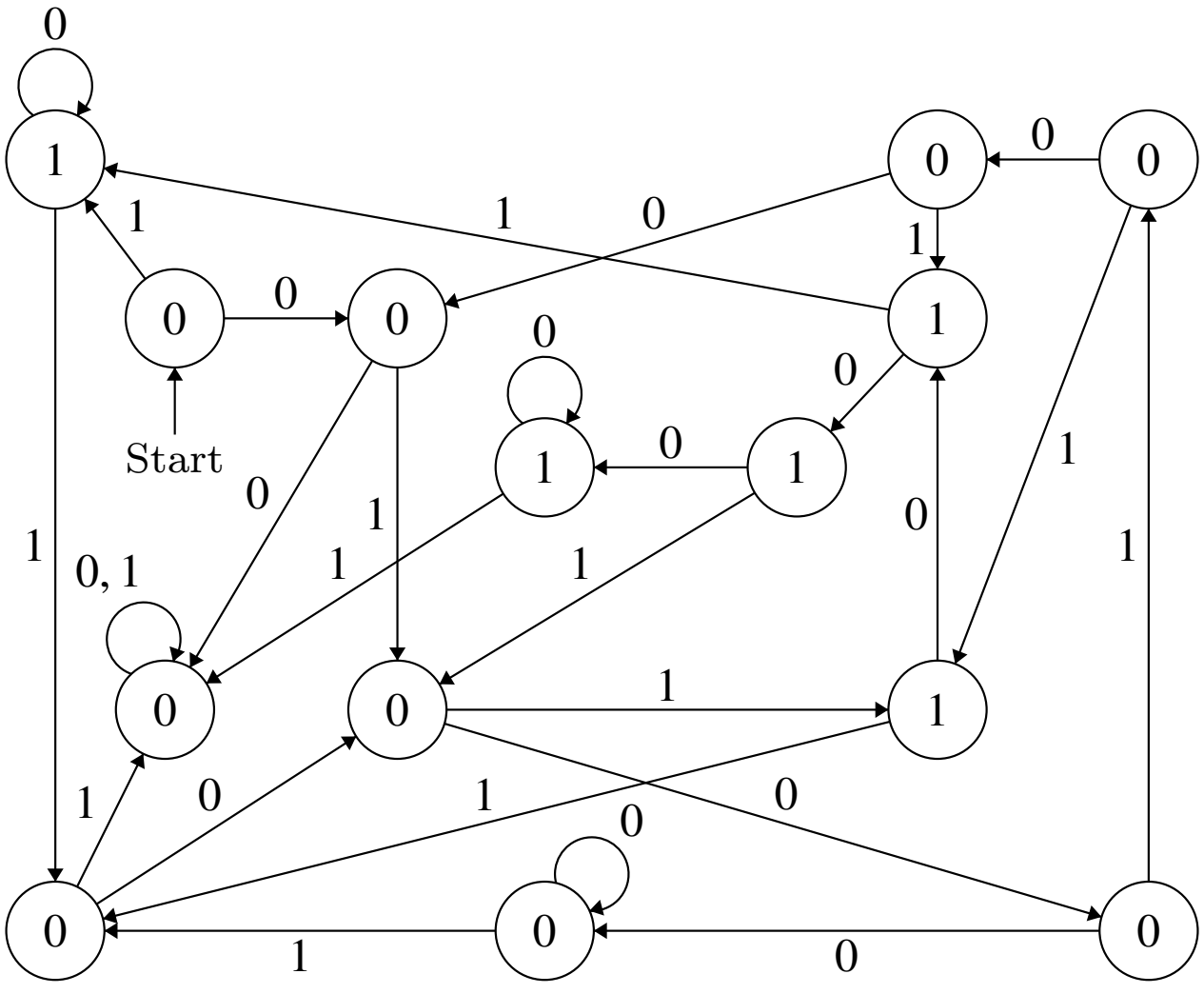
An automaton generating a power series of order 4 and break sequence $(1, 5)$



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

Theorem (Cobham, 1972)

Let $L \subset \Sigma^*$ be a regular language. Then L has either polynomial or exponential growth:

1. either $\#\{w \in L \mid |w| \leqslant n\} \geqslant c^n$ for some real $c > 1$ and large n;
2. or $\#\{w \in L \mid |w| \leqslant n\} \leqslant n^r$ for some integer r.

Sparseness

Theorem (Cobham, 1972)

Let $L \subset \Sigma^*$ be a regular language. Then L has either polynomial or exponential growth:

1. either $\#\{w \in L \mid |w| \leqslant n\} \geqslant c^n$ for some real $c > 1$ and large n;
2. or $\#\{w \in L \mid |w| \leqslant n\} \leqslant n^r$ for some integer r.

We call an algebraic power series

$$\sigma = \sum_{n \geqslant 0} a_n t^n$$

sparse if the associated language

$$L_\sigma = \{\mathrm{rep}_p(n) \mid a_n \neq 0\}$$

has polynomial growth.

Examples

- The series of Scherr–Zieve is sparse:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k \geqslant 0} \left(t^{3 \cdot 2^k - 2} + t^{4 \cdot 2^k - 2} \right) = t + t^2 + t^4 + t^6 + t^{10} + t^{14} + t^{22} + t^{30} + \cdots$$

- The series of Chinburg–Symonds is not. But it is a product of a sparse series and a rational function.

Examples

- The series of Scherr–Zieve is sparse:

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k \geqslant 0} \left(t^{3 \cdot 2^k - 2} + t^{4 \cdot 2^k - 2} \right) = t + t^2 + t^4 + t^6 + t^{10} + t^{14} + t^{22} + t^{30} + \cdots$$

- The series of Chinburg–Symonds is not. But it is a product of a sparse series and a rational function.
- The series $\sigma_{\min}$ is of neither of these types.

In 2019 Albayrak and Bell gave a valuation-theoretic and Galois-theoretic characterisation of sparse power series.

Sparse representatives

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.

Sparse representatives

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.

1. Any power series of order 2 and break sequence (1) is conjugate to the sparse power series whose support consists of the integers whose base-2 representation is either 1^μ or $1^\mu 0$ for some $\mu \geqslant 1$.

Sparse representatives

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.

1. Any power series of order 2 and break sequence (1) is conjugate to the sparse power series whose support consists of the integers whose base-2 representation is either 1^μ or $1^\mu 0$ for some $\mu \geqslant 1$.
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 whose support consists of the integers whose base-2 representation is either 1 or $10^{\mu-1}(10^{\mu-2})^\ell 0$ for some $\mu \geqslant 2$, $\ell \geqslant 0$.

Sparse representatives of automorphisms of order 2

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 whose support 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.

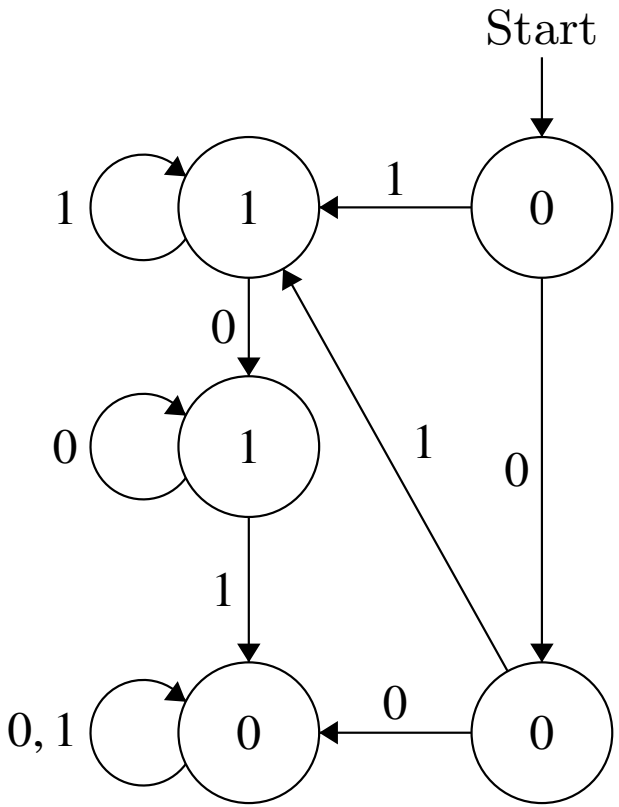
Sparse representatives of automorphisms of order 2

Theorem (continued)

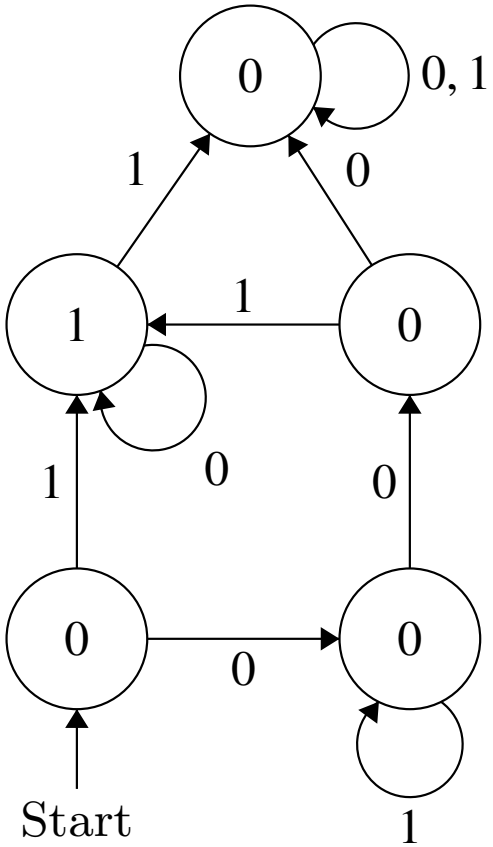
3 If $m = 2^\mu + 1$, then any power series of order 2 and break sequence (m) is conjugate to the sparse power series whose support consists precisely of the integers $m(\ell - 1) + 1$ with $\ell \geqslant 1$ an integer whose base-2 expansion contains at most μ occurrences of the digit 1 and all these 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).

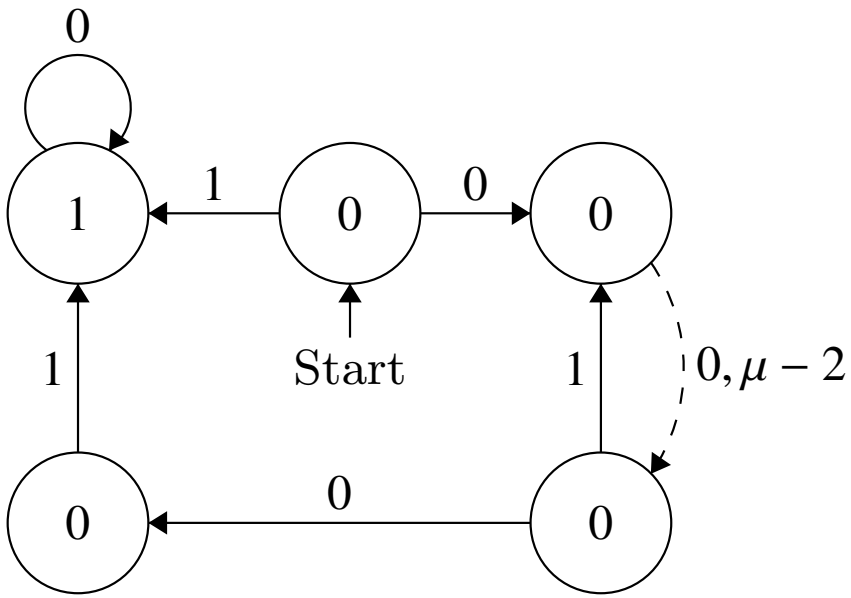
The automaton generating a sparse power series of order 2 and break sequence 1



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



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



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

- Are the 'p-automata of finite order' somehow special from an automaton-theoretic point of view?

Open questions

- Are the 'p-automata of finite order' somehow special from an automaton-theoretic point of view?
- 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.

Open questions

- Are the 'p-automata of finite order' somehow special from an automaton-theoretic point of view?
- 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.
- 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.