From de Bruijn graphs to automorphisms of the shift

Peter J. Cameron, University of St Andrews
(joint with Collin Bleak and Feyisayo Olukoya)

Ural Workshop on Group Theory and Combinatorics
28 August 2020

2020
UWGTC

Automata

A (finite-state, deterministic) automaton is a machine with a finite set S of internal states; when it reads a symbol from a given finite input alphabet A it changes its state in a deterministic way.

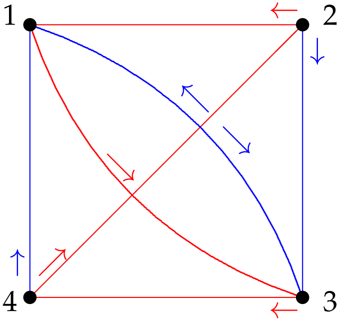
An automaton can be represented by an edge-labelled directed graph whose vertices are the states, edge-labels corresponding to the symbols in the alphabet, so that there is an arc with label a from s to t if reading symbol a causes the machine to change from state s to state t.

Thus we require that *there is a unique arc with any given label leaving any vertex*.

If the machine reads the symbols of a word in order, it undergoes the concatenation of the corresponding transitions. So we can also regard the automaton as a transformation monoid (a submonoid of the full transformation monoid on S) with a prescribed set of generators.

An example

Here is a 4-state automaton, with alphabet consisting of two letters Blue and Red.



The word (Blue, Red, Blue) moves from state 2 to 3 to 4 to 1. You can check that this word takes you to state 1 no matter where you start.

Synchronization

A word with the property we just saw (that it maps the automaton to a fixed state no matter what its initial state) is called a reset word. In other words, in the corresponding transformation semigroup, a reset word is a word in the generators which evaluates to a transformation of rank 1, that is, one whose image has cardinality 1.

An automaton which possesses a reset word is called synchronizing.

There is a polynomial-time algorithm to decide whether an automaton is synchronizing. However, finding the shortest reset word is more difficult!

The Černý conjecture

One of the oldest and most difficult problems in automata theory is the Černý conjecture:

> *If an n-state automaton is synchronizing, then it has a reset word of length at most $(n-1)^2$.*

It is known that the bound $(n-1)^2$ would be best possible; there are synchronizing automata which have no shorter reset word than this.
After more than half a century , the best upper bound known is $O(n^3)$. The Černý conjecture is known to be true in some special cases. It has stimulated a lot of research in many areas including extremal combinatorics and permutation groups.
But I won't discuss it any further here!

Strong synchronization

For what follows, I require a much stronger condition.

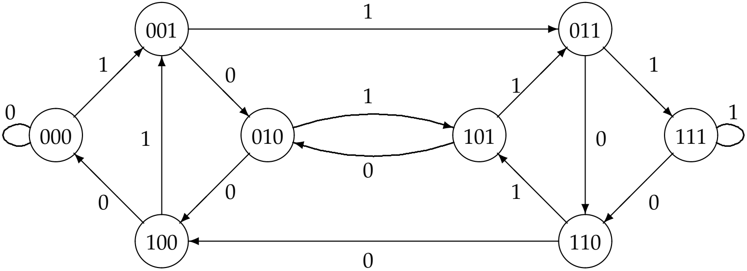
An automaton is strongly synchronizing at level n if, when it reads a word w of length n, the final state depends only on w and not on the initial state.

In other words, an automaton is strongly synchronizing at level n if every word of length n is a reset word.

This condition, as we will see, is closely connected with automorphisms of the shift map in symbolic dynamics.

De Bruijn graphs

Let n be a positive integer and A a finite alphabet. The de Bruijn graph $G(n, A)$ has vertex set A^n. For $a \in A$, $w \in A^n$, the target of the edge labelled a with source w is obtained by removing the first letter of w and appending a.
Here is $G(3, \{0, 1\})$:



The de Bruijn graph as automaton

Clearly the de Bruijn graph satisfies the condition to be an automaton: there is a unique arc with any given label leaving any vertex.

Regarded as an automaton, $G(n, A)$ is strongly synchronizing at level n: for if it reads a word $w = a_1 \cdots a_n$ of length n, the letters in the label of the initial state all drop off the front, and the final state is labelled by w.

It seems clear that it is in some sense the "universal" automaton which is strongly synchronizing at level n. We now turn to this.

Foldings

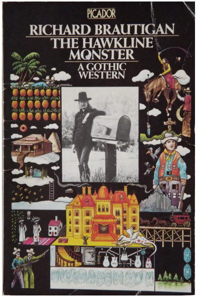
A folding of an automaton is an equivalence relation $\equiv$ on the set of states having the property that, if states s and t are equivalent, and s' and t' are the states resulting from reading a given letter a from these two states, then s' and t' are equivalent. If $\equiv$ is a folding of an automaton $\mathcal{A}$, then there is a folded automaton $\mathcal{A}/\equiv$ whose states are the equivalence classes of states in $\mathcal{A}$, the transition functions defined in the obvious way. The defining condition guarantees that these are well-defined. The following are now easy to see.

- If $\mathcal{A}$ is strongly synchronizing at level n, then so is any folding of $\mathcal{A}$.
- Any automaton which is strongly synchronizing at level n over the alphabet A is a folding of $G(n, A)$.

Problem

If $|A| = k$, how many foldings of $G(n, A)$ are there?

Counting foldings



> “I count a lot of things that theres no need to count,” Cameron said. “Just because that’s the way I am. But I count all the things that need to be counted.”
>
> Richard Brautigan, *The Hawkline Monster: A Gothic Western*

I believe that if you properly understand objects of some kind, you should be able to count them.

How many foldings of the de Bruijn graph with word length n over an alphabet of size q are there?

The problem of counting foldings seems to be very difficult. We have solved it only for $n \leq 2$ and a couple of sporadic cases.
The case $n = 1$ is trivial. The de Bruijn graph $G(1, A)$ has vertex set A, and for every $a \in A$, an edge labelled a from each vertex to the the vertex a. So any partition of A gives rise to a folding. So the number of foldings is $B(|A|)$, the Bell number.
I will give a brief sketch of the case $n = 2$. To recap: vertices of the graph are ordered pairs of letters, which we will write as xy; there is an edge labelled a from xy to ya. A folding is an equivalence relation on the vertex set such that
$xy \equiv uv \Rightarrow ya \equiv va$.
We have not even been able to extend the formula to the case $n = 3$.

Theorem

Let

$$R(s,t) = \sum_{\tau} (-1)^{|\tau|-1} (|\tau|-1)! \prod_{i=1}^{|\tau|} B(a_i s),$$

where τ runs over all partitions of $\{1,\ldots,t\}$, $|\tau|$ is the number of parts of τ, and a_i is the size of the ith part.

Then the number of foldings of $G(2,A)$ is

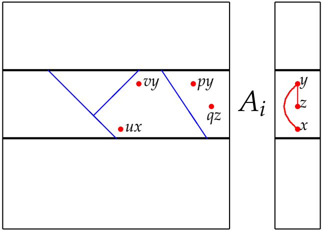
$$\sum_{\pi} \prod_{i=1}^{|\pi|} R(|\pi|,|A_i|),$$

where the sum is over all partitions $\pi = \{A_1,\ldots,A_{|\pi|}\}$ of A.

The formula looks complicated, but is easy to calculate; the numbers grow quite fast. For $|A| = 2,\ldots,7$, the values are 5, 192, 78721, 519338423, 82833228599906, 429768478195109381814.

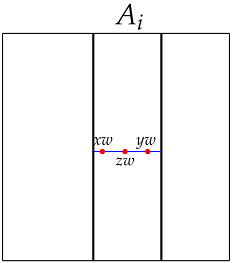
Sketch proof

Define a graph Γ on the alphabet A, two vertices x and y joined if there exist u and v such that $ux \equiv vy$ (this implies that $xw \equiv yw$).



Let π be the partition of A into connected components of Γ. If A_i is a part of Γ, then the set $A \times A_i$ (the horizontal stripe in the figure) is a union of parts of the folding: no part can cross into a different horizontal stripe.

Moreover, by the definition of a folding, we see that if $x, y \in A_i$, then xw and yw lie in the same part of the folding.

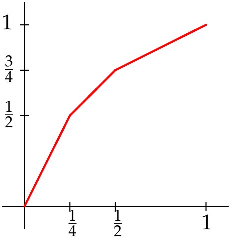


So the sets $A \times A_i$ can be treated independently, and within such a set, points with the same second coordinate and with first coordinates within the same part of π belong to the same part. So we have to count partitions of $\pi \times A_i$ for each part A_i of π. There is no proper non-empty subset B of A_i such that $\pi \times B$ is a union of sets of the folding. So inclusion-exclusion gives the nuber of possiblities on $A \times A_i$ to be $R(|\pi|, |A_i|)$. Multiply and sum over π.

Thompson's groups

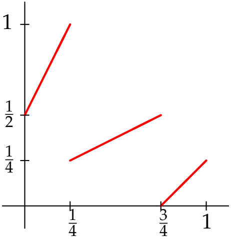
Three of the best-studied infinite groups were discovered by Richard Thompson in the 1950s, and are known as F, T and V. Here are brief descriptions.

The group F consists of piecewise-linear order-preserving permutations of the unit interval, where the slopes are powers of 2 and the points of discontinuity of the slope are dyadic rationals.



Representing numbers in the unit interval by dyadic rationals, we see that the group acts by prefix replacement: in the above example, $00x \mapsto 0x$, $01x \mapsto 10x$, $1x \mapsto 11x$.

The group T is similar but preserves the circular order of the roots of unity.
However our main interest lies in the group V, where the order-preserving assumption is dropped and arbitrary prefix replacement is allowed, provided only that the resulting map is a bijection.



In product replacement form this is $00x \mapsto 1x$, $01x \mapsto 010x$, $10x \mapsto 011x$, and $11x \mapsto 00x$.

The Higman–Thompson groups

The group V is a finitely presented infinite simple group, the first known example of such a group.

The construction was generalised by Graham Higman to give a two-parameter family of such groups, denoted by $G_{n,r}$. (Each is finitely presented, and is simple or has a simple subgroup of index 2.) They can be defined by product replacement as above; the alphabet $\{0,1\}$ is replaced by an alphabet of n symbols, and the parameter r indicates that at the first step we choose one of r initial symbols chosen from a different alphabet.

Pardo showed that $G_{n,r} \cong G_{m,s}$ if and only if $m = n$ and $\gcd(r, n-1) = \gcd(s, m-1)$.

Transducers

To relate these groups to the previous discussion, we introduce the notion of a transducer: this is an automaton which has the capacity to write as well as read symbols from an alphabet. In general, a transducer reads a symbol, changes state, and writes a string of symbols from the alphabet (possibly empty).

In order to avoid trivial cases, we always assume that *when a transducer reads an infinite string of symbols, it writes out an infinite string*: in other words, if we traverse a cycle in the digraph of the underlying automaton, at least one symbol is written.

As just hinted, a transducer A with a prescribed starting state s (called an initial transducer) can be regarded as defining a map from the set A^ω of infinite strings over the alphabet A to itself. We are interested in the case where this map is invertible, and the inverse is also represented by a transducer.

The rational group

The rational group $\mathcal{R}_n$ over an n-letter alphabet A was defined by Grigorchuk, Nekrashevych, and Suschanskiĭ.
It is the group of invertible transformations of A^ω induced by initial transducers.
The maps are composed in the usual way; we can define a composition directly on transducers by using the output of the first transducer as input to the second.
The definition can be extended to the group $\mathcal{R}_{n,r}$, which acts on strings where the first symbol is taken from an auxiliary alphabet of size r.

The automorphism group of $G_{n,r}$

An invertible initial transducer is said to be bisynchronizing if the underlying automaton is strongly synchronizing, and the same holds for the automaton representing its inverse.

Theorem

The automorphism group of $G_{n,r}$ is the group of transformations of A^ω induced by bisynchronizing initial transducers; so it is a subgroup of the rational group $\mathcal{R}_{n,r}$.

This theorem is proved in the paper of Bleak, Cameron, Maissel, Navas and Olukoya (arXiv 1605.09302).

Consequences

I mention here two consequences of this analysis.

Theorem

The outer automorphism group of $G_{n,r}$ has trivial centre and unsolvable order problem.

The proof involves a connection between $\mathrm{Out}(G_{n,r})$ and the automorphism group of the two-sided shift in symbolic dynamics, allowing known results about the second to be transferred to the first. I turn now to this.

Shift maps

The shift map σ comes in two flavours. It acts on either the set A^ω of infinite strings of symbols from A, or on the set $A^{\mathbb{Z}}$ of two-way infinite strings; it moves each symbol one place to the left. (In the one-way case, the first symbol of the string is lost, so the shift is onto but not one-to-one; in the second case it is a bijection.)

For example, if $A = \{0, 1\}$ and we interpret A^ω as the set of binary decimals representing the unit interval, then the shift map is the function $x \mapsto 2x \pmod 1$.

The shift map is the central character in *symbolic dynamics*, arising from a discretisation of dynamics of (for example) planetary orbits.

Automorphisms of the shift

An automorphism of the shift is a homeomorphism of X^ω or $X^\mathbb{Z}$ (regarded as Cantor space) which commutes with σ.

The connection between automata and automorphsims of the shift was pointed out by Grigorchuk *et al.* in 2000.

Automorphisms of the one-sided shift are given by transducers; in the case of the two-sided shift, we will see that a little more is required.

Two recent papers by Bleak, Cameron and Olukoya (arXiv 2004.08478 and 2006.01466) use transducers to study the automorphism groups of the shift maps. Some of the results are new; several give simpler proofs of known results, or versions more suitable to actual computation. Here are some examples.

First, it is noted that the automorphism group of the one-sided shift over an n-letter alphabet embeds into the group of outer automorphisms of $G_{n,r}$: the automorphisms are given by bisynchronizing transducers.

In the one-sided case, the orders of torsion elements of $\mathrm{Aut}(\sigma)$ are orders of automorphism groups of foldings of de Bruijn graphs.

In the two-sided case, $\mathrm{Aut}(\sigma)$ contains the group generated by σ as a central subgroup; the quotient is embeddable in the group of outer automorphisms of $G_{n,r}$.

In this case, automorphisms are specified by an annotated transducer, where the transducer determines the coset of $\langle\sigma\rangle$, and the annotation determines the element of this coset.

References

Collin Bleak, Peter Cameron, Yonah Maissel, Andrés Navas, and Feyishayo Olukoya, The further chameleon groups of Richard Thompson and Graham Higman: Automorphisms via dynamics for the Higman groups $G_{n,r}$, arXiv 1605.09302.

Collin Bleak, Peter Cameron and Feyishayo Olukoya, Automorphisms of shift spaces and the Higman–Thompson groups: the one-sided case, arXiv 2004.08478.

Collin Bleak, Peter Cameron and Feyishayo Olukoya, Automorphisms of shift spaces and the Higman–Thompson groups: the two-sided case, arXiv 2006.01466.

R. I. Grigorchuk, V. V. Nekrashevych, V. I. Sushchanskiĭ, Automata, dynamical systems and groups, *Tr. Mat. Inst. Steklova*, **231** (2000), 134–214; English version *Proc. Steklov Inst. Math.* **231** (2000), 128–203.

… for your attention.