Permutation groups and synchronizing automata

Peter J. Cameron

p.j.cameron@qmul.ac.uk

Bridging The Gaps
7 November 2008

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

We can force the machine to make any desired sequence of transitions (each transition being a mapping from the set of states to itself).

Automata

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed.

We can force the machine to make any desired sequence of transitions (each transition being a mapping from the set of states to itself).

We can represent an automaton as an edge-coloured directed graph, where the vertices are the states, and the colours are the transitions. We require that the graph should have exactly one edge of each colour *leaving* each vertex.

Synchronization

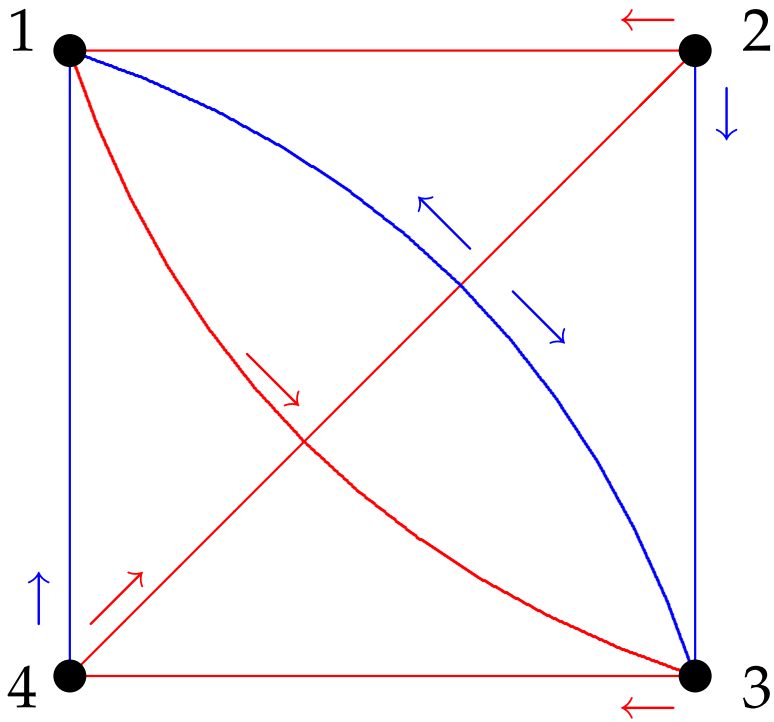
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

Synchronization

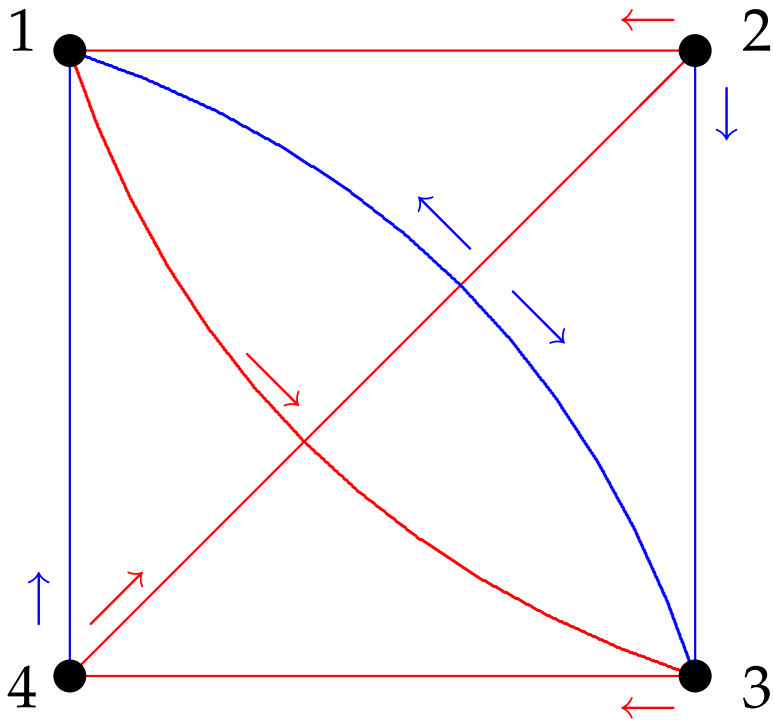
Suppose that you are given an automaton (whose structure you know) in an unknown state. You would like to put it into a known state, by applying a sequence of transitions to it. Of course this is not always possible!

A reset word is a sequence of transitions which take the automaton from any state into a known state; in other words, the composition of the corresponding transitions is a constant mapping.

An example



An example



You can check that (Blue, Red, Blue, Blue) is a reset word which takes you to room 3 no matter where you start.

Applications

- Industrial robotics: pieces arrive to be assembled by a robot. The orientation is critical. You could equip the robot with vision sensors and manipulators so that it can rotate the pieces into the correct orientation. But it is much cheaper and less error-prone to regard the possible orientations of the pieces as states of an automaton on which transitions can be performed by simple machinery, and apply a reset word before the pieces arrive at the robot.

Applications

- Industrial robotics: pieces arrive to be assembled by a robot. The orientation is critical. You could equip the robot with vision sensors and manipulators so that it can rotate the pieces into the correct orientation. But it is much cheaper and less error-prone to regard the possible orientations of the pieces as states of an automaton on which transitions can be performed by simple machinery, and apply a reset word before the pieces arrive at the robot.
- Bioinformatics: If a soup of DNA molecules is to perform some computation, we need the molecules to be all in a known state first. We can simultaneously apply a reset word to all of them, where the transitions are induced by some chemical or biological process.

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

Problem

Suppose that an n-vertex automaton has a reset word. Show that it has one of length at most $(n-1)^2$.

The Černý conjecture

How do we decide whether a reset word exists? We can search for one by trial and error; how far do we have to go before we can conclude that there is no reset word?

Problem

Suppose that an n-vertex automaton has a reset word. Show that it has one of length at most $(n-1)^2$.

This is the Černý conjecture, and is still open. If true, the bound would be best possible.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

Proposition

A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

A group-theoretic approach

At the other extreme from a synchronizing automaton is one in which all the transitions are permutations (and generate a permutation group). One approach to the Černý conjecture is to separate out this difficulty.

A permutation group G on a set Ω is said to be synchronizing if, whenever $f : \Omega \to \Omega$ is a mapping which is not a permutation, the semigroup generated by G and f contains a reset word (a constant mapping).

Proposition

A permutation group G on Ω is non-synchronizing if and only if there is a non-trivial partition π of Ω and a subset Δ of Ω such that, for all $g \in G$, Δg is a section (of transversal) of π.

Corollary

A synchronizing group is primitive.

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ is the cardinality of the largest complete subgraph of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Graph-theoretic characterisations

These properties can be detected by undirected graphs admitting the group G. The clique number $\omega(X)$ is the cardinality of the largest complete subgraph of X; the chromatic number $\chi(X)$ is the smallest number of colours required to colour the vertices so that adjacent vertices get different colours. Clearly $\omega(X) \leq \chi(X)$, since vertices of a complete subgraph must get different colours.

Proposition

Let G be a permutation group on Ω, with $|\Omega| = n$. Then G is non-synchronizing if and only if there is a non-trivial G-invariant graph X for which $\omega(X) = \chi(X)$.

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?
Let f be a non-permutation. Without loss of generality, a reset word will look like

$$fg_1fg_2f\cdots fg_{r-1}f$$

for $g_1,\ldots,g_r \in G$. We need to bound r and also the expressions for $g_1,\ldots,g_r$ in terms of generators.

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?
Let f be a non-permutation. Without loss of generality, a reset word will look like

$$fg_1fg_2f\cdots fg_{r-1}f$$

for $g_1,\ldots,g_r \in G$. We need to bound r and also the expressions for $g_1,\ldots,g_r$ in terms of generators.
Suppose that G is "large" enough that, whatever set S is the image of $fg_1f\cdots fg_{i-1}f$, we can always move it by an element $g_i \in G$ to a position where f will not act one-to-one on it. Then the image can be made strictly smaller with each application of f, and we have $r \leq n-1$.

Towards the Černý conjecture

Suppose that G is a synchronizing permutation group. What further properties do we need in order that the Černý conjecture should hold for any automaton obtained by adjoining a non-permutation to a set of generators of G?
Let f be a non-permutation. Without loss of generality, a reset word will look like

$$fg_1fg_2f\cdots fg_{r-1}f$$

for $g_1,\ldots,g_r \in G$. We need to bound r and also the expressions for $g_1,\ldots,g_r$ in terms of generators.
Suppose that G is "large" enough that, whatever set S is the image of $fg_1f\cdots fg_{i-1}f$, we can always move it by an element $g_i \in G$ to a position where f will not act one-to-one on it. Then the image can be made strictly smaller with each application of f, and we have $r \leq n-1$.
Arnold and Steinberg proved the Černý conjecture in some special cases by this method.