# Combinatorial problems from transformation semigroups

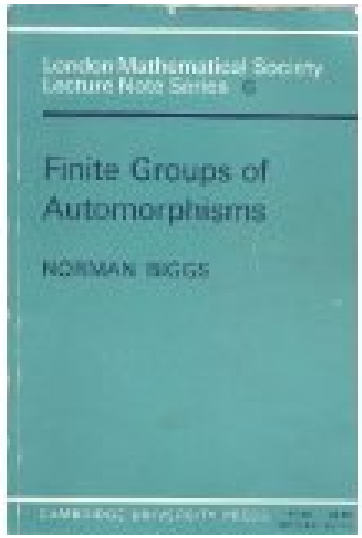
Peter J. Cameron

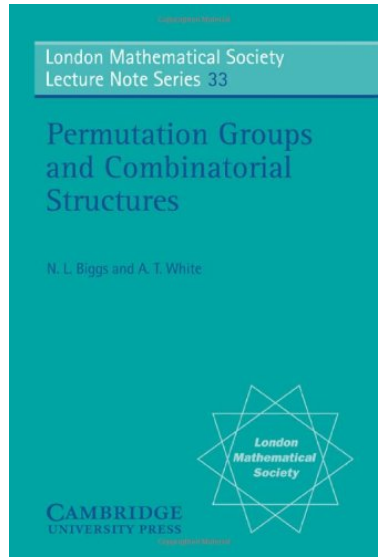
University of St Andrews

The Norman Biggs Lecture
London Combinatorics Colloquia
LSE, 15 May 2014

# Norman Biggs

Norman has worked on many things. What I am talking about today could be regarded as a development from his book *Finite Groups of Automorphisms* (or *Permutation Groups and Combinatorial Structures*, as it became).




I strongly agree with the philosophy expressed in this book: objects with the most symmetry are likely to be the most interesting!

# Symmetry

The Oxford English Dictionary gives four meanings of the word symmetry:

1. The quality of being made up of exactly similar parts facing each other or around an axis.
2. Correct or pleasing proportion of the parts of a thing.
3. Similarity or exact correspondence between different things.
4. A law or operation where a physical property or process has an equivalence in two or more directions.

None of these quite captures the use of symmetry in mathematics, though the first comes close. The second definition is much too general, while the fourth refers to symmetry in physics.
Somewhere buried in these definitions is the idea that symmetry refers to correspondence between parts of an object, not a global property of the object.

# Symmetry and algebra

Group theory is traditionally the branch of algebra which studies symmetry. A bijective correspondence from an object to itself which preserves its structure is an automorphism, or symmetry, of the object. The collection of all symmetries (in this sense) is a group, more particularly a permutation group. But if we consider a symmetry as a correspondence between parts, we are led to the notion of a semigroup, in two guises:

- a transformation semigroup, a set of maps on a given set $X$ which is closed under composition;
- an inverse semigroup of partial bijections, a set of bijections between subsets of $X$ closed under composition (where the composition is defined on any point $x$ whose image under the first map lies in the domain of the second.

# Inverse semigroups

Most of this talk will be about transformation semigroups. But let me begin with some combinatorics of inverse semigroups, from a paper by Laradji and Umar.
The symmetric inverse semigroup consists of all partial bijections on a set $X$ of size $n$. Its cardinality is

$$\sum_{k=0}^{n} \binom{n}{k}^2 k!,$$

an interesting combinatorial sequence but not one which has been very much studied. (It is number A002720 in the On-Line Encyclopedia of Integer Sequences.)
Laradji and Umar defined some sub-semigroups of this semigroup, by taking $X = \{1, 2, \ldots, n\}$, with its natural order.

# Some interesting numbers

## Theorem (Laradji and Umar)

- *The semigroup of all order-preserving partial bijections on* $\{1, \ldots, n\}$ *has order* $\binom{2n}{n}$.
- *The semigroup of decreasing partial bijections has order* $B_{n+1}$, *and the semigroup of strictly decreasing partial bijections has order* $B_n$, *where* $B_n$ *is the n-th Bell number.*
- *The semigroup of decreasing order-preserving partial bijections has order* $C_{n+1}$, *and the semigroup of monotone strictly decreasing partial bijections has order* $C_n$, *where* $C_n$ *is the n-th Catalan number.*

Laradji and Umar also found interpretations of the Fibonacci, Stirling, Schröder, Euler, Lah and Narayana numbers in counting problems about inverse semigroups.

# Abstract algebra and enumerative combinatorics

We learn something when we can interpret combinatorial numbers as orders of algebraic structures, especially groups. Lagrange's Theorem means that group orders tend to have a rich arithmetic structure.
I first learned from Norman's paper on chip-firing games the fact that the number of spanning trees of a graph is the order of an abelian group canonically associated with the graph (a reduced homology group).
For the complete graph $K_n$, this group is the direct product of $n-2$ copies of the cylic group of order $n$.

# Endomorphisms and automorphisms

Rather than an order, we can impose algebraic structure on the set $X$, and ask for maps which are endomorphisms, or partial maps which are partial isomorphisms.
This is not well explored yet, but here is a curiosity.

## Theorem

*The number of partial isomorphisms of rank $k$ of an $n$-dimensional vector space over a field of order $q$ is equal to the number of endomorphisms of rank $k$ of the same vector space.*

## Corollary

*The order of the inverse semigroup of partial isomorphisms of an $n$-dimensional vector space of rank $n$ over a field of order $q$ is equal to the order of the semigroup of endomorphisms, namely $q^{n^2}$.*

# A proof

The result on the preceding slide holds because, for a linear map $f$, once we have specified the kernel of $f$, the set of vectors mapped to zero by $f$, then the partition into inverse images of the points in the image is just the partition into cosets of the kernel. So to choose an endomorphism of $V$ of rank $k$, we have to specify its image $W$ (a subspace of $V$ of dimension $k$), its kernel $U$ (a subspace of dimension $n-k$), and an isomorphism from $V/U$ to $W$.

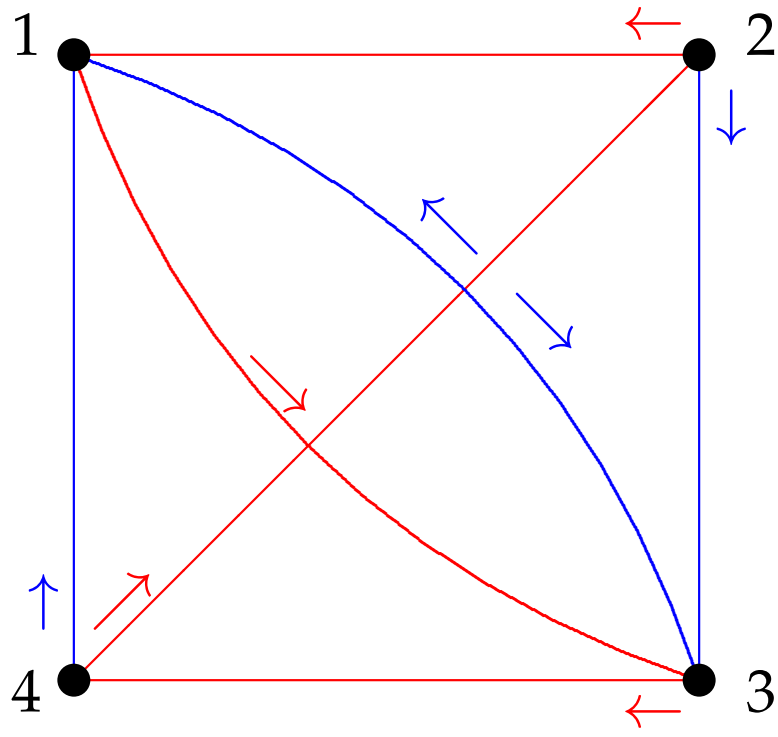
Now to choose a partial isomorphism of rank $k$, we have to specify the domain and codomain (two subspaces of dimension $k$) and an isomorphism between them.

So the theorem follows from the fact that the numbers of subspaces of dimension $k$ and $n-k$ in an $n$-dimensional vector space are equal (by duality).

# Synchronization

A transformation semigroup $S$ is synchronizing if it contains an element of rank 1.
The notion comes from automata theory. An automaton is a machine which responds to an input symbol from an alphabet $A$ by undergoing a prescribed change of state. It can be represented by a directed graph whose vertices are the states, and with arcs labelled by symbols from $A$, so that each vertex has a unique arc with each possible label leaving it. The transitions which result from reading a word in the alphabet $A$ form a transformation semigroup on the set of states.
Now an automaton is synchronizing if there is a word $w$ in the letters of $A$ such that, if the automaton reads $w$, then it reaches a fixed state, independent of its starting state.

# An example




You can check that (Blue, Red, Blue, Blue) takes you to state 3 no matter where you start.

# The Černý conjecture

One of the oldest open problems in automata theory is the Černý conjecture, according to which if an $n$-state automaton is synchronizing then there is a reset word of length at most $(n-1)^2$.
It is known that this would be best possible (if true). However, after nearly 50 years of work, the best general upper bound for the length of the reset word is cubic in $n$.
I note in passing that, for a given automaton, deciding if it is synchronizing can be done in polynomial time, but finding the length of the shortest reset word is NP-hard.

# The obstruction to synchronization

An endomorphism of an undirected graph $\Gamma$ is a map from the vertex set of $\Gamma$ to itself which carries edges to edges. (Its effect on non-edges is unspecified.
The endomorphisms of a fixed graph form a transformation semigroup $\mathrm{End}(\Gamma)$. It is non-synchronizing if the graph has at least one edge.

**Theorem**

*A transformation semigroup $S$ is non-synchronizing if and only if there exists an undirected graph $\Gamma$ with the properties that*

- $S \leq \mathrm{End}(\Gamma)$;
- $\Gamma$ *has at least one edge;*
- $\omega(\Gamma) = \chi(\Gamma)$, *or equivalently, the core of* $\Gamma$ *is a complete graph.*

# Synchronizing groups

In an attack on the Černý conjecture, Ben Steinberg and João Araújo defined a permutation group $G$ to be synchronizing if the semigroup $\langle f, G\rangle$ is synchronizing for any non-permutation $f$.

It is known that a synchronizing group is primitive (preserves no non-trivial equivalence relation), and a doubly transitive group is synchronizing, but neither implication reverses.

Although testing an automaton for synchronization, and testing a group for primitivity or 2-transitivity, are all easy, testing a group for the synchronizing property appears to be hard. The best algorithm we have is: construct all the $G$-invariant graphs, and check each to see if its clique number and chromatic number are equal. The group is synchronizing if and only if all these checks fail.

Though lousy from a complexity viewpoint, this algorithm has been used on groups with degree in the thousands.

# Packing and covering

Let $t, k, n$ be positive integers with $t < k < n$. A $(t, k, n)$ packing, (resp. covering), is a collection $\mathcal{B}$ of $k$-subsets of an $n$-set with the property that every $t$-subset is contained in at most one (resp. at least one) member of $\mathcal{B}$.
A collection of $k$-sets which is both a packing and a covering (and hence a maximum packing and a minimum covering) is a Steiner system $S(t, k, n)$.
A recent spectacular preprint of Peter Keevash asserts that Steiner systems exist whenever the obvious necessary conditions (congruences on $n$) are satisfied and $n$ is "sufficiently large".

# Subsets and partitions

We turn now to a different but analogous context. Let $k$ and $n$ be positive integers with $k < n$.
A $k$-partition of an $n$-set $X$ is a partition $P$ of $X$ with $k$ parts. A $k$-subset $A$ of $X$ is a transversal, or section, for $P$ if it intersects every part of $P$ in a unique point.
In place of $t$-sets and $k$-sets with the relation of set inclusion, I am going to consider $k$-sets and $k$-partitions with the transversal relation.

# A combinatorial problem

We will see that the study of transformation semigroups leads naturally to various questions, of which the following is typical.

## Problem

*Let $k$ and $n$ be given, with $1 < k < n$. What is the smallest cardinality of a family of $k$-sets which includes a transversal for every $k$-partition?*

Asymptotic results on this problem for fixed $k$, or for $k = o(n^{1/3})$, were found by Bujtás and Tuza in 2009. However, exact results are mostly not known. Bujtás and Tuza remark that the problem for $k = n - 2$ is equivalent to finding the Turán number for graphs of girth 5. They say, "The exact determination of $f(n, k)$ appears to be far beyond reach to our present knowledge."

# Transformation semigroups

A transformation semigroup on a finite set $X$ is a set $S$ of maps $s : X \to X$ which is closed under composition. If every map in $S$ is bijective, then $S$ is a permutation group.
We write maps on the right of their arguments, and compose left-to-right.
Just as the set of all permutations of $X$ forms the symmetric group $S(X)$ on $X$, so the set of all transformations of $X$ forms the full transformation semigroup $T(X)$. If $X = \{1, 2, \ldots, n\}$, we write $S_n$ and $T_n$.
Thus, a transformation semigroup is a sub-semigroup of the full transformation semigroup.

# The normaliser

Semigroup theory is a generalisation of group theory, but applications of group theory to semigroup theory were hampered by the fact that a semigroup may not have a "group of units", or even an identity element.
However, for a transformation semigroup $S$ on $X$, there is a substitute, the normaliser of $S$, the group of all permutations $g$ of $X$ such that, for all $s \in S$, we have $g^{-1}sg \in S$. It is a permutation group.
Recent results indicate that the normaliser has a very strong influence on the structure of a transformation semigroup.
These results use the modern structure theory of permutation groups, based on the O'Nan–Scott theorem and using the Classification of Finite Simple groups where necessary.

# The connection

Let $s$ be an element of the full transformation semigroup $T_n$. The rank of $s$ is the cardinality of the image of $s$. The kernel of $s$ is the partition in which two points $i, j$ belong to the same part if and only if $is = js$; it is a $k$-partition, where $k$ is the rank of $s$.

## Proposition

*The rank of $s_1 s_2$ is equal to the number of parts of the kernel of $s_2$ which intersect the image of $s_1$.*

## Corollary

*Suppose the smallest rank of an element of the transformation semigroup $S$ is $k$. Let $s_1$ and $s_2$ be any two elements of $S$ having rank $k$. Then the image of $s_1$ is a transversal for the kernel of $s_2$, and vice versa.*

# The Livingstone–Wagner Theorem

A permutation group $G$ on $X$ is $k$-homogeneous if it acts transitively on the set of $k$-element subsets of $X$, and is $k$-transitive if it acts transitively on the set of ordered $k$-tuples of distinct elements of $X$.
In 1964, Livingstone and Wagner proved:

## Theorem (Livingstone–Wagner)

*Let $G$ be a $k$-homogeneous permutation group on a set of cardinality $n$, where $k \leq n/2$. Then*

- *$G$ is $(k-1)$-homogeneous;*
- *$G$ is $(k-1)$-transitive;*
- *if $k \geq 5$, then $G$ is $k$-transitive.*

The proof of the first part used character theory of the symmetric group, but can be formulated as a purely combinatorial argument.
Later Kantor determined the groups which are $k$-homogeneous but not $k$-transitive for $k = 2, 3, 4$. Following the Classification of Finite Simple Groups, we now know all the $k$-transitive groups for $k \geq 2$.

# The universal transversal property

A permutation group $G$ on $X$ has the $k$-universal transversal property if every orbit of $G$ on $k$-sets contains a transversal to every $k$-partition.

## Theorem (Araújo–Cameron)

*With a few known exceptions, a group of degree $n$ with the $k$-universal transversal property (for $k \leq n/2$) is $k$-homogeneous, and hence has the $(k-1)$-universal transversal property.*

This theorem is tantalisingly like the first part of Livingstone–Wagner, but our proof uses the Classification of Finite Simple Groups and obtains a nearly complete classification of such groups.

This has the surprising corollary that, if $G$ is a permutation group with the property that for all rank $k$ maps $f, f$ is regular in the semigroup $\langle f, G\rangle$ (that is, has a quasi-inverse), then *every* element of this semigroup is regular.

# Chains of (semi)groups

One of the most dramatic differences between semigroups and groups is that groups satisfy Lagrange's Theorem: the order of a subgroup $H$ of $G$ divides the order of $G$, so in particular $G$ is at least twice as large as $H$. So the length of a chain of subgroups in a group is at most logarithmic in the group order. By contrast, is is possible for a sub-semigroup $T$ of $S$ to contain all but one element of $S$, and so the only general bound for the length of a chain of sub-semigroups of $S$ is the order of $S$. This is attained if all products are zero, and in various other cases too.

# Chains in $S_n$ and $T_n$

As noted above, the length of a chain of subgroups in $S_n$ is at most $\log_2 n! \sim n \log n$. In fact the exact value is known:

**Theorem**

*The length of the longest subgroup chain in $S_n$ is*

$$\left\lceil \frac{3n}{2} \right\rceil - b(n) - 1,$$

*where $b(n)$ is the number of ones in the base 2 representation of $n$.*

The length of the longest chain of sub-semigroups in $T_n$ is not known precisely yet, but with Max Gadouleau and James Mitchell, I have shown that it is $\Omega(n^n)$.

# Some details

In $T_n$, the set $T_{n,k}$ of maps of rank at most $k$ forms an ideal (the analogue of a normal subgroup), so it is enough to deal with the quotient of successive ideals. We can identify $T_{n,k}/T_{n,k-1}$ with the set of maps of rank exactly $k$ together with a "zero" element, where the product of two maps in the quotient is zero if its rank is less than $k$.

Let $A$ be a $k$-set and $P$ a $k$-partition; let $T(P,A)$ be the set of maps with kernel $P$ and image $A$. (This set has cardinality $k!$ and is known to semigroup theorists as a D-class.) If $s_i \in T(P_i,A_i)$ for $i = 1,2$ and $A_1$ is not a transversal of $P_2$, then $s_1 s_2 = 0$ in the quotient.

So we can go up in steps of 1 as long as we have a collection $\mathcal{A}$ of $k$-sets and a collection $\mathcal{P}$ of $k$-partitions such that, for all $A \in \mathcal{A}$ and $P \in \mathcal{P}$, $A$ is not a transversal to $P$. We call such a pair a league of rank $k$.

# A problem

## Problem

*Given $k$ and $n$, what is the maximum of $|\mathcal{A}| \cdot |\mathcal{P}|$ over all leagues of rank $k$ on an $n$-set?*

This maximum number, multiplied by $k!$, is a lower bound for the length of a chain in the quotient $T_{n,k}/T_{n,k-1}$, so summing these over $k$ gives a lower bound for the length of a chain in $T_n$. [Some improvements are also possible.]
These ideas lead to a linear lower bound for the length of $T_n$, namely $n^n/e^2$. This is the subject of a forthcoming paper with Max Gadouleau, James Mitchell and Yann Peresse.

# Appendix: a problem

This appendix describes a problem I posed at the start of the lecture. It is an old problem about graphs with a high degree of regularity (the kind that Norman likes), but I wonder whhether modern techniques for dealing with large graphs might be applied,
We are looking for graphs with the following properties ($r$ is a positive integer):

- There are $(2r+1)^2(2r^2+2r-1)$ vertices.
- Each vertex has $2r^3(2r+3)$ neighbours.
- Two adjacent vertices have $r(2r-1)(r^2+r-1)$ common vertices.
- Two non-adjacent vertices have $r^3(2r+3)$ common neighbours.

## Problem

*Show that there exists $r_0$ such that there is no such graph with $r > r_0$.*

# The context

For a positive integer $k$, a graph is $k$-tuple regular if, for any set $X$ of vertices with $|X| \leq k$, the number of common neighbours of $X$ depends only on the isomorphism type of the induced subgraph on $X$.

Thus "1-tuple regular" means "regular", while "2-tuple regular" means "strongly regular". There are many such graphs. However, the only 5-tuple regular graphs are disjoint unions of complete graphs, complete multipartite graphs, the 5-cycle, and the line graph of $L(K_{3,3})$. What happens for $k = 3$ and $k = 4$?

It is known that a graph is 4-tuple but not 5-tuple regular if and only if it has the properties of the problem on the preceding slide.

Two exampes are known: $r = 1$ (the intersection graph of the 27 lines in a general cubic surface) and $r = 2$ (a graph admitting McLaughlin's sporadic simple group).