Permutation Groups and Transformation Semigroups

Peter J. Cameron
School of Mathematics and Statistics
University of St Andrews
North Haugh
St Andrews, Fife KY16 9SS
UK
pjc20@st-andrews.ac.uk

Contents

Preface

These notes accompany a course on Permutation Groups and Transformation Semigroups, given at the University of Vienna in March 2017. I am grateful to Tomack Gilmore for inviting me to give the lectures and facilitating the course, and to the University for its hospitality.

The last decade has seen some significant advances in the theory of finite transformation semigroups. One person responsible above all for these developments (and certainly for getting me interested in the subject) is João Araújo in Lisbon. Current progress relies heavily on the Classification of Finite Simple Groups (CFSG for short). The proof of this theorem is extremely long and difficult, but its application is not so mysterious, and part of the aim here is to show how consequences of CFSG can be brought to bear on these problems. In addition, a variety of combinatorial methods, ranging from graph endomorphisms to Ramsey's Theorem, have been used.

An important part of this area is synchronization theory. This arose in the early days of automata theory, and one of the oldest conjectures in automata theory, the *Černý conjecture*, is still unproved. It may be that the techniques described here will form part of the proof of this fascinating conjecture; but, even if they do not, a very interesting research area has been created.

To keep the notes self-contained, I have included brief introductions both to semigroup theory and to permutation groups. The next two chapters form the heart of the notes: one on synchronization, and one on other properties of semigroups such as regularity and idempotent generation. The emphasis is on how properties of the group of units influence the semigroup. The final chapter is not too strongly related. In the early 1980s, a remarkable formula was found for the length of the

longest chain of subgroups in the symmetric group S_n, namely

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

where $b(n)$ is the number of ones in the base 2 expansion of n. Recently this formula has been extended to the symmetric inverse semigroup, and some results for the full transformation semigroup obtained; I will discuss these.

The notes end with a discussion of open problems and further reading.

CHAPTER 1

Introduction to semigroups

I will assume some familiarity with the theory of groups. (If you need more information, I gave a crash course in group theory in Lisbon last November, and the notes are available.) However, I will begin at the beginning in the discussion of semigroups. For more information, see the book by Howie listed in the last chapter of the notes.

1.1 Basic concepts

We begin with the definitions.

- A *semigroup* is a set S with a binary operation $\circ$ satisfying the *associative law*:
$$a \circ (b \circ c) = (a \circ b) \circ c$$
for all $a, b, c \in S$.
- A *monoid* is a semigroup with an *identity* 1, an element satisfying
$$a \circ 1 = 1 \circ a = a$$
for all $a \in S$.
- A *group* is a monoid with *inverses*, that is, for all $a \in S$ there exists $b \in S$ such that
$$a \circ b = b \circ a = 1.$$

From now on we will write the operation as *juxtaposition*, that is, write ab instead of $a \circ b$, and a^{-1} for the inverse of a.

There is essentially no difference between semigroups and monoids: any monoid is a semigroup, and conversely, to any semigroup we can add an identity without violating the associative law. However, there is a very big difference between semigroups and groups:

Order	1	2	3	4	5	6	7	8
Groups	1	1	1	2	1	2	1	5
Monoids	1	2	7	35	228	2237	31559	1668997
Semigroups	1	5	24	188	1915	28634	1627672	3684030417

A semigroup which will occur often in our discussions is the *full transformation semigroup* T_n on the set $\{1,\ldots,n\}$, whose elements are all the maps from $\{1,\ldots,n\}$ to itself, and whose operation is composition. This semigroup is a monoid: the identity element is the identity map on $\{1,\ldots,n\}$. It contains the *symmetric group* S_n, the group of all permutations (bijective maps). Note that $T_n \setminus S_n$ is a semigroup.

The order of T_n is $|T_n| = n^n$.

In semigroups of maps, we always write the map to the right of its argument, and compose maps from left to right: thus $(xf)g$ is the result of applying first f and then g to the element $x \in \{1,\ldots,n\}$, which is equal to $x(fg)$ (the result of applying fg to x), by definition. (This is not the associative law, though it looks like it!)

1.2 Special semigroups

The most interesting semigroups are usually those which are (in some sense) closest to groups.

An element a of a semigroup S is *regular* if there exists $x \in S$ such that $axa = a$. The semigroup S is *regular* if all its elements are regular. Note that a group is regular, since we may choose $x = a^{-1}$.

Regularity is equivalent to a condition which appears formally to be stronger:

Proposition 1.1 *If $a \in S$ is regular, then there exists $b \in S$ such that $aba = a$ and $bab = b$.*

Proof Choose x such that $axa = a$, and set $b = xax$. Then

$$aba = axaxa = axa = a,$$
$$bab = xaxaxax = xaxax = xax = b.$$

□

Proposition 1.2 *The semigroup T_n is regular.*

Proof Given a map a, choose a preimage s for every t in the image of a, and define x to map t to s if t is in the image of a (arbitrary otherwise). □

An *idempotent* in a semigroup S is an element e such that $e^2 = e$. Note that, if $axa = a$, then ax and xa are idempotents. In a group, there is a unique idempotent, the identity.

Idempotents have played an important role in semigroup theory. One reason for this is that they always exist in a finite semigroup:

Proposition 1.3 *Let S be a finite semigroup, and $a \in S$. Then some power of a is an idempotent.*

Proof Since S is finite, the powers of a are not all distinct: suppose that $a^m = a^{m+r}$ for some $m, r > 0$. Then $a^i = a^{i+tr}$ for all $i \geq m$ and $t \geq 1$; choosing i to be a multiple of r which is at least m, we see that $a^i = a^{2i}$, so a^i is an idempotent. □

It follows that a finite monoid with a unique idempotent is a group. For the unique idempotent is the identity; and, if $a^i = 1$, then a has an inverse, namely a^{i-1}.

A semigroup S is an *inverse semigroup* if for each a there is a unique b such that $aba = a$ and $bab = b$. The element b is called the *inverse* of a. Among several other definitions, I menion just one: it is a semigroup S in which, for every $a \in S$, there is an element $a' \in S$ such that

$$(a')' = a, \quad aa'a = a \quad aa'bb' = bb'aa'$$

for all $a, b \in S$. Thus an inverse semigroup is a regular semigroup in which idempotents commute. (For this we need to show that every idempotent has the form aa'.) In an inverse semigroup, we often write a^{-1} for a'.

Proposition 1.4 *Let S be an inverse semigroup.*

(a) Each element of S has a unique inverse.

(b) The idempotents form a semilattice under the order relation $e \leq f$ if $ef = fe = f$.

1.3 Examples

The most famous inverse semigroup is the *symmetric inverse semigroup* on the set $\{1,\ldots,n\}$. Its elements are the *partial bijections* on this set, that is, all bijective maps $f : X \to Y$, where $X, Y \subseteq \{1,\ldots,n\}$. We compose elements wherever possible. Thus, if $f : X \to Y$ and $g : A \to B$, then fg is defined on the preimage (under f) of $Y \cap A$, and maps it to the image (under g) of this set. If $f : X \to Y$, then the inverse (as required in the definition of an inverse semigroup) is the inverse function, which maps Y to X: so ff^{-1} is the identity map on X, and $f^{-1}f$ the identity map on Y. This inverse semigroup is denoted by I_n. Its order is

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

since, for a map of rank k, there are $\binom{n}{k}$ choices for the domain and the same number for the rank, and $k!$ bijections between them.

Idempotents are just identity maps on subsets, and the semilattice of idempotents is simply the lattice of subsets of the set $\{1,\ldots,n\}$.

The formulae for the orders of the symmetric group ($|S_n| = n!$) and the full transformation semigroup ($|T_n| = n^n$) are simple and well-known. The order of the symmetric inverse semigroup is less familiar: it is sequence A002720 in the On-Line Encyclopedia of Integer Sequences, beginning

$$1, 2, 7, 34, 209, 1546, 13327, 130922, 1441729, 17572114, \ldots$$

Laradji and Umar [21] found that many familiar integer sequences can be represented as orders of "naturally-occurring" semigroups. Here are a few of them. We regard $\{1,\ldots,n\}$ as having its natural order. Here $\mathrm{Dom}(f)$ is the domain of the map f.

Consider the following three conditions on a partial bijection f of $\{1,\ldots,n\}$:

Monotonic: if $x, y \in \mathrm{Dom}(f)$ and $x < y$, then $xf < yf$;

Decreasing: if $x \in \mathrm{Dom}(f)$ then $xf \leq x$;

Strictly decreasing: if $x \in \mathrm{Dom}(f)$ then $xf < x$.

The set of partial permutations satisfying any collection of these conditions is a semigroup.

Let $P(n)$ be the number of partial permutations on $\{1,\ldots,n\}$. Denote the numbers of permutations which are respectively monotonic, decreasing, or strictly decreasing by a subscript m, d or s; we also allow combinations of subscripts. We saw the formula for $P(n)$ above. The other numbers are familiar combinatorial coefficients:

Theorem 1.5 *(a)* $P_m(n) = \binom{2n}{n}$.

(b) $P_d(n) = B_{n+1}$ *and* $P_s(n) = B_n$, *where* B_n *is the nth Bell number.*

(c) $P_{md}(n) = C_{n+1}$ *and* $P_{ms}(n) = C_n$, *where* C_n *is the nth Catalan number.*

Remark The *Bell number* B_n is the number of partitions of a set of n elements. It satisfies the recurrence

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k},$$

since we can choose a partition of $\{1,\ldots,n+1\}$ by first choosing the part containing $n+1$ (also containing, say, k points from $\{1,\ldots,n\}$), and then partitioning the remaining $n-k$ points arbitrarily. There is no simple formula for B_n.

The *Catalan number* C_n can be defined in many ways: for example, it is the number of ways of bracketing a non-associative product of $n+1$ terms. For $n=3$, for example, we have

$$((ab)c)d, (a(bc))d, (ab)(cd), a((bc)d), a(b(cd)).$$

Unlike the Bell number, there is a simple explicit formula for it:

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

The interpretation we use below is that in terms of *ballot sequences*; C_n is the number of ways of counting the votes in an election in which the two candidates A and B each receive n votes, on condition that candidate A is never behind in the count. The ballot sequences for $n=3$ are

ABABAB, ABAABB, AABBAB, AABABB, AAABBB.

Proof (a) Argue as above. Once the domain and range are chosen, there is a unique monotonic bijection between them. So

$$P_m(n) = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

by a standard binomial coefficient identity.

(b) We show first that $P_d(n) = P_s(n+1)$. If f is a decreasing partial permutation on $\{1,\ldots,n\}$, then the map g given by $g(x+1) = f(x)$ whenever this is defined is a strictly decreasing partial permutation on $\{1,\ldots,n+1\}$. The argument

reverses. This correspondence preserves the property of being monotonic, so also $P_{md}(n) = P_{ms}(n+1)$. Now we select a decreasing bijection by first choosing its fixed points, and then choosing a strictly decreasing bijection on the remaining points. If there are k fixed points, then there are $P_s(n-k)$ ways to choose the strictly decreasing bijection. So we have

$$P_s(n+1) = P_d(n) = \sum_{k=0}^{n} \binom{n}{k} P_s(n-k).$$

Thus, $P_s(n)$ satisfies the same recurrence as the Bell number B_n, and we have

$$P_s(n) = B_n, \qquad P_d(n) = B_{n+1}.$$

(c) The preceding proof fails for monotonic decreasing maps, since such a map cannot jump over a fixed point. Instead, we encode a strictly decreasing map by a ballot sequence.

Let f be monotonic and strictly decreasing on $\{1,\ldots,n\}$. We encode f by a sequence of length $2n$ in the alphabet consisting of two symbols A and B as follows. In positions $2i-1$ and $2i$, we put

AB, if $i \notin \mathrm{Dom}(f)$ and $i \notin \mathrm{Ran}(f)$,

BB, if $i \notin \mathrm{Dom}(f)$ and $i \in \mathrm{Ran}(f)$,

AA, if $i \in \mathrm{Dom}(f)$ and $i \notin \mathrm{Ran}(f)$,

BA, if $i \in \mathrm{Dom}(f)$ and $i \in \mathrm{Ran}(f)$.

It can be shown that this gives a bijective correspondence between the set of such functions and the set of *ballot sequences* of length $2n$. The proof is an exercise. (It is necessary to show that the resulting string has equally many As and Bs, and that each initial substring has at least as many As as Bs; and that every string with these properties can be decoded to give a strictly decreasing monotone function. The proof that the correspondence is bijective is then straightforward.)

It follows that $P_{ms}(n) = C_n$ (the nth Catalan number), and from the remark in part (b), also $P_{md}(n) = C_{n+1}$. □

Laradji and Umar have found that many other interesting counting sequences arise in calculating the orders of various inverse semigroups of partial bijections. Among these are Fibonacci, Stirling, Schröder, Euler, Lah and Narayana numbers.

There are linear analogues of some of the above semigroups. Let V be an n-dimensional vector space over the field of order q. The analogues of S_n, T_n and I_n are respectively

- the *general linear group* $\mathrm{GL}(n,q)$ of invertible $n \times n$ matrices;
- the *general linear semigroup* $M_n(q)$ of all $n \times n$ matrices;
- the inverse semigroup $I_n(q)$ of all linear bijections between subspaces of V.

The orders of the first two are well known:

- $|\mathrm{GL}(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$;
- $|M_n(q)| = q^{n^2}$.

In the third case, something rather surprising happens:

Proposition 1.6 *Let V be a finite vector space. Then the orders of the general linear semigroup on V and the inverse semigroup of linear bijections between subspaces are equal.*

Proof The proof uses the *Gaussian* or *q-binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$, which is defined to be

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-2)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-1)\cdots(q^n-q^{k-1})}.$$

For prime power q, this is equal to the number of k-dimensional subspaces of an n-dimensionanl vector space over the finite field $\mathrm{GF}(q)$ with q elements. It has several other interpretations, in the theories of lattice paths and quantum groups among others.

Let V be n-dimensional over the field of order q. Clearly the number of rank k linear bijections between subspaces is

$$\sum_{k=0}^{n} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^2 |\mathrm{GL}(k,q)|.$$

To choose a linear map of rank k from V to V, we have to choose a kernel U (a subspace of dimension $n-k$), an image W (a subspace of dimension k) and an isomorphism from V/U to W. So the order of this semigroup is

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ n-k \end{bmatrix}_q \begin{bmatrix} n \\ k \end{bmatrix}_q |\mathrm{GL}(k,q)|.$$

Since $\begin{bmatrix} n \\ n-k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q$ by duality, the result follows. (In more detail: there is a bijection between the sets of k-dimensional subspaces of V and of $(n-k)$-dimensional subspaces of its dual space V^*, which pairs each subspace of V with its annihilator in V^*.) □

Remark The proof also gives us the identity

$$\sum_{k=0}^{n} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q \right)^2 |\mathrm{GL}(k,q)| = q^{n^2},$$

an interesting example of a q-identity which has no analogue for sets (since, for example, $|T_3| = 27$ but $|I_3| = 34$).

Research problem Let A be a finite group. Let $S_1(A)$ denote the semigroup of endomorphisms of A, and $S_2(A)$ the inverse semigroup of isomorphisms between subgroups of A.

If A is abelian, then it satisfies duality (the dual group of A is its group of *characters*, or homomorphisms to the multiplicative group of non-zero complex numbers, and the proof above shows that $|S_1(A)| = |S_2(A)|$.

Is it true that, for any non-abelian group A, we have $|S_1(A)| \neq |S_2(A)|$?

1.4 Analogues of Cayley's theorem

Cayley's Theorem asserts that a group of order n is isomorphic to some subgroup of S_n. The proof is well-known: we take the *Cayley table* of the group G, the matrix (with rows and columns labelled by group elements); each column of the Cayley table (say the column indexed by b) corresponds to a transformation ρ_b of the set G (taking the row label a to the product ab, the ath element of column b). Then it is straightforward to show that

- ρ_b is a permutation, so that $\rho_b \in S_n$;
- the map $b \mapsto \rho_b$ is one-to-one;
- the map $b \mapsto \rho_b$ is a homomorphism.

So the set $\{\rho_b : b \in G\}$ is a subgroup of S_n isomorphic to G.

This theorem has an important place in the history of group theory. In the nineteenth century, the subject changed from descriptive (the theory of *transformation groups* or *permutation groups*) to axiomatic; Cayley's theorem guarantees that the "new" abstract groups are the same (up to isomorphism) as the "old" permutation groups or subgroups of S_n.

Almost the same is true for semigroups:

Proposition 1.7 *Any semigroup of order n is isomorphic to a subsemigroup of the full transformation semigroup T_{n+1}.*

Proof If we follow the proof of Cayley's theorem, the thing that could go wrong is the second bullet point: the map $b \mapsto \rho_b$ may not be one-to-one. To fix the problem, we first add an identity element to the semigroup, and then follow Cayley's proof. Now, if $\rho_b = \rho_c$ and 1 is the identity, then

$$b = 1b = 1\rho_b = 1\rho_c = 1c = c,$$

so the map $b \mapsto \rho_b$ is one-to-one. □

For inverse semigroups, there is a similar representation theorem. The proof is a little more complicated, and is not given here.

Theorem 1.8 (Vagner–Preston Theorem) *Let S be an inverse semigroup of order n. Then S is isomorphic to a sub-semigroup of the symmetric inverse semigroup I_n.*

Interesting inverse semigroups arise in the following way. Let L be a meet-semilattice of subsets of $\{1,\ldots,n\}$ invariant under the permutation group G. Then the restrictions of elements of G to sets in L form an inverse semigroup. For an example, we can take G to be the projective group $\mathrm{PGL}(d,q)$ acting on the points of the projective space, and L the lattice of flats of the projective space; or, analogously, the affine group and the lattice of flats of the affine space. As far as I know, these semigroups have not been much investigated.

1.5 Basics of transformation semigroups

We discuss a few concepts related to transformations and transformation semigroups on a finite domain Ω.

Any map $f : \Omega \to \Omega$ has an *image*

$$\mathrm{Im}(f) = \{xf : x \in \Omega\},$$

and a *kernel*, the equivalence relation $\equiv_f$ defined by

$$x \equiv_f y \Leftrightarrow xf = yf,$$

or the corresponding partition of Ω. (We usually refer to the partition when we speak about the kernel of f, which is denoted $\mathrm{Ker}(f)$.) The *rank* $\mathrm{rank}(f)$ of f is the cardinality of the image, or the number of parts of the kernel.

Under composition, we clearly have

$$\mathrm{rank}(f_1 f_1) \leq \min\{\mathrm{rank}(f_1), \mathrm{rank}(f_2)\},$$

and so the set $S_m = \{f \in S : \text{rank}(f) \leq m\}$ of elements of a transformation semigroup which have rank at most m is itself a transformation semigroup. In general, there is no dual concept; but the set of permutations in S (elements with rank n) is closed under composition, and forms a permutation group (which is the group of units of S), if it happens to be non-empty. The interplay between permutation groups and transformation semigroups is central to these lectures.

Suppose that f_1 and f_2 are transformations of rank r. As we saw, the rank of $f_1 f_2$ is at most r. Equality holds if and only if $\text{Im}(f_1)$ is a *transversal*, or *section*, for $\text{Ker}(f_2)$, in the sense that it contains exactly one point from each part of the partition $\text{Ker}(f_2)$. This combinatorial relation between subsets and partitions is crucial for what follows. We note here one simple consequence.

Proposition 1.9 *Let f be a transformation of Ω, and suppose that $\text{Im}(f)$ is a section for $\text{Ker}(f)$. Then some power of f is an idempotent with rank equal to that of f.*

Proof The restriction of f to its image is a permutation, and some power of this permutation is the identity. □

CHAPTER 2

Permutation groups

I will go briefly through the standard introductory material on permutation groups. More detail can be found in the book by Dixon and Mortimer in the bibliography.

One of the biggest changes in the landscape of finite group theory has been the Classification of Finite Simple Groups, whose result was announced in 1980 but whose proof was not completed until about 2010. A *simple group* is a group in which the only normal subgroups are the whole group and the identity. The Classification can be stated as follows:

Theorem 2.1 (CFSG) *A finite simple group is one of the following:*

(a) a cyclic group of prime order;

(b) an alternating group A_n, for $n \geq 5$;

(c) a group of Lie type;

(d) one of 26 *sporadic simple groups.*

The alternating group A_n consists of all even permutations of $\{1,\ldots,n\}$. A *group of Lie type* is closely related to a matrix group; there is one family associated with every simple Lie algebra over the complex numbers (these are the *Chevalley groups*), together with some variants called *twisted groups*. These groups include the classical groups (symplectic, orthogonal and unitary) as well as various exceptional families. The *sporadic groups* fall into no general pattern, and usually an *ad hoc* construction is required for each group.

The easiest and perhaps most important of the groups of Lie type are the *projective special linear groups* $\mathrm{PSL}(n,q)$. This group has the form $\mathrm{SL}(n,q)/Z$,

where $\mathrm{SL}(n,q)$ is the *special linear group*consisting of all $n \times n$ matrices of determinant 1 over $\mathrm{GF}(q)$, and Z is its centre (consisting of the scalar matrices in $\mathrm{SL}(n,q)$). It is simple for all $n \geq 2$ and all q except for the two cases $\mathrm{PSL}(2,2)$ and $\mathrm{PSL}(2,3)$, which are isomorphic to S_3 and A_4 respectively.

The *Jordan–Hölder Theorem* asserts that any finite group G has a series of subgroups

$$G = G_0 > G_1 > \cdots > G_r = \{1\},$$

called a *composition series*, in which each group G_i is a normal subgroup of its predecessor and G_{i-1}/G_i is simple; moreover, the multiset of isomorphism types of simple groups is independent of the particular composition series chosen. In other words, simple groups are the "building blocks" for all groups. Although we understand the building blocks, the procedure for fitting them together (*extension theory*) is still rather mysterious. Nevertheless, CFSG has had a huge impact on finite group theory and related areas of algebra, combinatorics and computer science.

CFSG is an enormously powerful tool for studying finite groups. However, in order to apply it, we need very little information about how it is proved. Much more important is detailed knowledge of the groups appearing in the theorem, and in particular, their subgroups, matrix representations, and the kinds of structure that they act on. For this, see the books by Wilson and by Taylor listed in the final chapter. We are particularly interested in permutation groups, and for these we refer to the books by Cameron and by Dixon and Mortimer.

2.1 Transitivity and primitivity

We are particularly interested in *primitive* permutation groups. Their definition and importance stem from a couple of reductions which attempt to show that certain properties of permutation groups need only be checked for primitive groups.

2.1.1 Orbits and transitivity

The orbit decomposition for a permutation group is a generalisation of the well-known cycle decomposition for a permutation. Let G be a permutation group on Ω. Define a relation $\equiv_G$ by the rule that $a \equiv_G b$ if there exists $g \in G$ with $ag = b$. This is an equivalence relation (the reflexive, symmetric and transitive laws follow directly from the identity, inverse and closure laws for G), and so Ω is the disjoint union of sets Δ called *orbits*; G is *transitive* if it has just one orbit.

If G is an intransitive permutation group, with orbits $\Delta_1, \Delta_2, \ldots$, let G_i be the permutation group induced on Δ_i by G. The groups G_i (a permutation group on Δ_i)

are the *transitive constituents* of G. Then G is a subgroup of the direct product of the groups G_i; indeed, it is a *subdirect product*, that is, a subgroup which projects onto G_i under the natural projection of the direct product onto a factor, for all i.

The algorithm for finding the orbits of a permutation group is a simple extension of the algorithm for decomposing a single permutation into disjoint cycles. It can be expressed as follows. Suppose we are given generators $g_1, \ldots, g_n$ of a permutation group. Form a directed graph with edges (x, xg_i) for all $x \in \Omega$ and $i = 1, \ldots, n$. Then the connected components of this digraph are the orbits.

2.1.2 Blocks and primitivity

Let us say that a structure on a set Ω is *trivial* if it is invariant under the symmetric group on Ω. For example, the only trivial subsets are the empty set and the whole of Ω; and G is transitive if and only if it fixes no non-trivial subset of Ω.

We can adopt a similar approach for the next definition. The only trivial partitions of Ω are the partition into singletons and the partition whose only part is Ω. Now we say that the transitive permutation group G on Ω is *primitive* if it fixes no non-trivial partition of Ω. Note that we only define primitivity for transitive groups.

If the group G is imprimitive, a non-trivial G-invariant partition of Ω is a *system of imprimitivity*, and its elements are *blocks of imprimitivity*.

As for intransitive groups, the study of imprimitive groups can be reduced to that of smaller primitive groups. Suppose that B is a system of imprimitivity for G, and $\Delta \in B$. Let H be the group induced on the set Δ by its setwise stabiliser in G, and K the group induced on B by G. Then G can be embedded in the *wreath product* $H \wr K$. To define this group, note that all parts in the partition B of Ω have the same size, and conjugation in G transfers the action of H on Δ to its action on any block. Now the wreath product is the group generated by

- the direct product of $|B|$ copies of H, indexed by B; and
- the group K, permuting the copies of Δ.

The structure theorem says that the original group G is embedded in a natural way in the wreath product $H \wr K$.

Any finite group has a faithful action as a transitive permutation group (this is the content of Cayley's Theorem). However, the structure of primitive groups is more restricted. For example, it is known that a primitive group has at most two minimal normal subgroups; if there are two, then they are isomorphic to each other. Our next goal is the *O'Nan–Scott Theorem*, which gives a much more

precise description of primitive groups. But first we need one more reduction, in the same spirit as the two we have already seen.

If G is imprimitive, they we may embed it into the wreath product of two transitive groups of smaller degree. Repeating this refinement we eventually reach primitive groups, called *primitive components* of G, amd find that G is an iterated wreath product of primitive groups. However, unlike the Jordan–Hölder theorem, the primitive components may depend on the decomposition chosen. Here is an example.

We let G be the symmetric group S_4, acting on the set of 12 ordered pairs of distinct elements from $\{1,2,3,4\}$. The group G is transitive. It is imprimitive in various ways:

- G preserves the equivalence relation whose classes are a pair and its reverse. There are 6 equivalence classes, indexed by the unordered pairs or 2-element subsets. This action is also imprimitive, with three equivalence classes each consisting of two disjoint unordered pairs. The group induced on the three classes is S_3. So G is embedded in the iterated wreath product of C_2, C_2 and S_3.
- G preserves the equivalence relation where two pairs are equivalent if they have the first componenent. There are four equivalence classes, indexed by the common first component, and G permutes them as the natural action of S_4, which is primitive. The stabiliser of a class is S_3, which has its natural action on the elements of that class. So G is contained in the wreath product of S_3 and S_4.

2.1.3 Cartesian structures and basic groups

A *Cartesian structure* on a finite set Ω is a bijection between Ω and A^n, the set of all n-tuples over a set A, where $|A| > 1$ and $n > 1$. In other words, it is an identification of Ω with the set of n-tuples, or words of length n, over the alphabet A.

The set A^n has a natural structure as an *association scheme*, known as the *Hamming scheme*. This is a partition of the set of pairs of n-tuples into n classes, the ith class consisting of pairs whose *Hamming distance* is i, where the Hamming distance between two n-tuples is the number of coordinates in which their entries differ. Thus, a Cartesian structure on Ω is the same as a Hamming scheme. Hamming schemes play an important role in coding theory, first highlighted by Delsarte, but we will not be considering them further here. The book by Bailey has more information on association schemes.

A primitive permutation group G on Ω is called *non-basic* if it preserves a Cartesian structure (or Hamming scheme) on Ω, and is *basic* otherwise.

Suppose that G preserves the Cartesian structure A^n. Then G induces a permutation group on the set of n coordinates, which we call K; moreover, the stabiliser of a coordinate (say, the first) induces a permutation group on the set A of symbols occurring in that coordinate, which we call H. Now it turns out that G is embedded in a natural way in the wreath product $H \wr K$. Note, however, that this is a completely different action of the wreath product from the one defined earlier. We call the previous action the *imprimitive action* of the wreath product, and the present one the *product action*.

For example, the wreath product of the symmetric groups of degrees 3 and 2 is a group of order $(3!)^2 \cdot 2! = 72$; the imprimitive action is as the automorphism group of the complete bipartite graph $K_{3,3}$, and the product action is as the automorphism group of the 3×3 grid graph (which can also be regarded as the *line graph* of $K_{3,3}$).

2.2 The O'Nan–Scott Theorem

The O'Nan–Scott Theorem can be separated into two parts. One part relates the minimal normal subgroup of a non-basic primitive group G to that of the group H defined earlier. The second, which is more important to us, tells us what basic groups look like.

First we look at three particular types of primitive group.

- An *affine group* is a permutation group G acting on a vector space V and having the form

$$G = \{x \mapsto xA + b : A \in H, b \in V\},$$

  where H is a group of invertible linear maps from V to itself (that is, a subgroup of the *general linear group* $\mathrm{GL}(V)$ of all invertible linear maps on V). An affine group is always transitive, since it has a normal subgroup consisting of translations,

$$T = \{x \mapsto x + b : b \in V\},$$

  which acts transitively on V. It can be shown that G is a primitive permutation group if and only if H is an *irreducible* linear group (preserves no non-empty proper subspace of V), while G is basic if and only if H is a *primitive linear group*, that is, an irreducible linear group which preserves no non-trivial direct sum decomposition of V.

- A *diagonal group* is one which has a normal subgroup of the form T^r, where T is a non-abelian finite simple group, acting on the coset space of its diagonal subgroup
$$D(T^r) = \{(t,t,\ldots,t) : t \in T\}.$$
In the case $r = 2$, this normal subgroup has a simpler description: we can identify the domain with the group T, and T^2 acts by left and right translation:
$$(g,h) : x \mapsto g^{-1}xh.$$

- A group G is *almost simple* if $T \leq G \leq \mathrm{Aut}(T)$ for some non-abelian finite simple group T. (The group T is embedded into its own automorphism group as the group of all *inner automorphisms*, maps of the form $x \mapsto g^{-1}xg$; the name reflects the fact that, for any finite simple group T, the group $\mathrm{Aut}(T)/T$ is "small" (a consequence of the Classification of Finite Simple Groups). Note that, unlike the other two cases, we say nothing at all about the way that G acts; we can have any faithful primitive action of G.

Theorem 2.2 (O'Nan–Scott Theorem) *Let G be a basic primitive permutation group. Then G is affine, diagonal or almost simple.*

Obviously CFSG is immediately applicable to the study of diagonal and almost simple groups. It is also relevant to affine groups, since the linear subgroup H is often close to being simple.

2.3 Multiply transitive groups

A group G is *t-transitive* on Ω if it acts transitively on the set of ordered t-tuples of distinct elements of Ω; and is *t-homogeneous* if it acts transitively on the set of t-element subsets of Ω.

The symmetric group S_n is n-transitive, while the alternating group A_n is $(n-2)$-transitive. (There are just two permutations which map a given $(n-2)$-tuple to another; they differ by a transposition, which is an odd permutation, so one of them lies in the alternating group. Note that t-transitivity gets stronger as t increases, so knowledge of the 2-transitive groups would in principle determine all the multiply transitive groups.

Clearly a t-transitive group is t-homogeneous. The converse is, in some sense, almost true. Since t-homogeneity is equivalent to $(n-t)$-homogeneity, we may assume without loss of generality that $t \leq n/2$. Now Livingstone and Wagner [24] showed:

Theorem 2.3 *For $5 \leq t \leq n/2$, a t-homogeneous group is t-transitive.*

Livingstone and Wagner also showed that, for $t \leq n/2$, a t-homogeneous group is $(t-1)$-transitive. The t-homogeneous but not t-transitive groups for $t = 2,3,4$ were determined by Kantor [18, 19].

None of the above results require CFSG (though Kantor's result uses the *Feit–Thompson theoreom* on solubility of groups of odd order). By contrast, what follows relies on CFSG; at present there is no prospect of an alternative proof.

Burnside proved the special case of the O'Nan–Scott theorem for 2-transitive groups: such a group G has a unique minimal normal subgroup, which is either elementary abelian (whence G is affine) or simple (whence G is almost simple). So there are two strands to the classification of 2-transitive groups. Both were handled in the 1980s; many people, including Hering, Kantor, Liebler, Saxl, and especially Liebeck, contributed. See, for example, [17, 20, 22, 23].

I will not give the list here; this can be found in, for example, the book by Dixon and Mortimer.

2.4 Groups and graphs

Let G be a permutation group on Ω. In the 1960s, Donald Higman in the USA and Boris Weisfeiler in the USSR introduced methods for studying G based on its action on Ω^2, the set of ordered pairs of elements of Ω. They extracted from this action a combinatorial object which Higman called a *coherent configuration*, giving rise to a semisimple associative algebra over $\mathbb{C}$ which Weisfeiler called a *cellular algebra*. (The term "cellular algebra" is now used with a completely different meaning, so the term "coherent configuration" has now become standard.) Coherent configurations generalise a concept introduced in statistics, *association schemes*.

We will not need the full machinery of coherent configurations, nor its algebraic aspects. Something simpler will suffice, the notion of G-invariant graphs on the vertex set Ω. We assume in this section that the group G is transitive on Ω.

The set of 2-element subsets of Ω has a natural action of G, and splits into orbits $O_1, O_2, \ldots, O_s$ for some s. For any subset I of $\{1,\ldots,s\}$, we can take the union of the sets O_i for $i \in I$ as the edge set of a graph. Since G maps each set O_i to itself, it acts as a group of automorphisms of the graph, which we will call Γ_I. We call the graphs Γ_i (for $1 \leq i \leq s$) the *orbital graphs* of G.

Proposition 2.4 *A graph on the vertex set Ω admits G as a group of automorphisms if and only if it is Γ_I for some $I \subseteq \{1,\ldots,s\}$.*

For example, let G be the cyclic group of order 5, acting on the set $\{1,2,3,4,5\}$ in the natural way. The set of 2-subsets falls into two orbits, $O_1 = \{12,23,34,45,51\}$ and $O_2 = \{13,24,35,41,52\}$ (where we use ij for the 2-subset $\{i,j\}$). So there

are four G-invariant graphs: the two 5-cycles with edge sets O_1 and O_2, the null graph, and the complete graph.

Since G is transitive, each G-invariant graph is regular. Primitivity can also be recognised. The following result is very important to us. It was first observed by Higman.

Proposition 2.5 *The transitive group G on Ω is primitive if and only if every non-null G-invariant graph on Ω is connected; or, equivalently, if every orbital graph for G is connected.*

Proof If there is a non-null G-invariant graph which is not connected, then its connected components form a G-invariant partition, and so G is imprimitive. Conversely, suppose that G is imprimitive, with a non-trivial invariant partition P, and let x, y be points in the same part of P. Then every image of $\{x,y\}$ under G consists of two points in the same part of P. So the orbital graph with edge set $\{x,y\}^G$ is non-null and disconnected. □

If G is 2-homogeneous, there is a single G-orbit on 2-sets, and so the only G-invariant graphs are complete and null. But, if G is not 2-homogeneous, then there is necessarily a G-invariant graph which is neither complete nor null.

The *rank* of a permutation group G on Ω is defined to be the number of G-orbits on Ω^2 – these orbits are called *orbitals*. If G is transitive, one of these orbitals consists of all the pairs (x,x) for $x \in \Omega$, the so-called *diagonal orbital*. Any orbit of G on 2-sets corresponds to either one or two non-diagonal orbitals on Ω^2 (one orbital if there is a pair in the orbital whose points are interchanged by an element of G – these are the *self-paired orbitals* – and two if not). So, if r is the rank, and s the number of G-orbits on 2-sets, then we have

$$r-1 \leq s \leq (r-1)/2.$$

For example, in the case of the cyclic group of order 5, the rank is 5, and all four non-diagonal orbitals are non-self-paired.

2.5 Consequences of CFSG

CFSG has many implications for group theory. For example, it implies the truth of *Schreier's conjecture*: the outer automorphism group of a finite simple group (that is, automorphisms modulo the normal subgroup of conjugations) is soluble. So one simple group cannot act non-trivially on another.

It has been used in many other areas, for example Babai's recent quasi-polynomial bound for the complexity of graph isomorphism.

I will look briefly at some of the consequences of CFSG, especially those which are interesting for transformation semigroup theory.

First and foremost are the classification theorems. We already mentioned that all the 2-transitive groups are known as a result of CFSG, and hence all the t-transitive groups for larger t. In particular, the following holds:

Theorem 2.6 (uses CFSG) *The only t-transitive groups for $t \geq 6$ are the symmetric and alternating groups; the only additional 5-transitive groups are the Mathieu groups M_{12} and M_{24}, and the only additional 4-transitive groups are M_{11} and M_{23}.*

There are also many classifications of primitive groups satisfying some extra conditions. (There are probably too many primitive groups for a complete classification ever to be feasible.) One such extra condition is "small degree". All the primitive groups of degree at most 4095 are known, and lists of these groups are included in the computer algebra systems Magma and GAP.

Another important classification is of the *rank* 3 primitive groups, where rank is as defined earlier, the number of orbits on ordered pairs. Let G have rank 3. If G has odd order then the other two orbits are *paired*, in the sense that reversing the ordered pairs in one orbit gives the other; thus G is 2-homogeneous. Otherwise, G is contained in the automorphism group of a complementary pair of graphs. Using CFSG, all such groups have been determined, (by Kantor, Liebler, Liebeck, and others): see [20, 22, 23].

Another consequence is that primitive groups are relatively small (with known exceptions). If we define a *large* primitive group to be either a symmetric or alternating group acting on k-subsets of the domain for fixed k, or a non-basic group contained in $H \wr K$ where H is a large basic primitive group of the type previously described, then the best result on the orders of primitive groups is due to Maróti [25]:

Theorem 2.7 (uses CFSG) *Let G be a primitive permutation group of degree n which is not large (as just defined). Then either G is a Mathieu group, or $|G| \leq n^{1+\log_2 n}$.*

2.6 Bases

A *base* for G is a sequence $(a_1, a_2, \ldots, a_b)$ of points of the domain whose pointwise stabiliser in G is the identity. Bases are important in computational group theory, since an element of G is uniquely determined by its effect on a base. Thus, it is an advantage to have as small a base as possible. Also, if G has degree n and has a base of size b, then $|G| \leq n(n-1)\cdots(n-b+1) \leq n^b$; so small bases are connected with small order as in the last result.

To choose a base for a permutation group, simply pick points and stabilise] them until you reach the identity. A point which is already fixed by the stabiliser of those already chosen is unnecessary, and a base containing such a point is called *redundant*. Clearly then any base of smallest size will be irredundant.

By the Orbit-Stabiliser Theorem, if H_i is the stabiliser of the first i points, then the index of H_{i+1} in H_i is equal to the size of the H_i-orbit containing a_{i+1}. So the obvious "greedy" strategy to find a small base is to choose a_{i+1} from an H_i-orbit of maximum size. (There may be more than one such orbit.) A base chosen in this way is called a *greedy base*.

Theorem 2.8 *Let G be a permutation group whose smallest base has size b. Then*

(a) an irredundant base has size at most $b\log_2 n$;

(b) a greedy base has size at most $b(\log\log n + c)$, where c is an absolute constant.

There is no simple computational method to find a base of minimal size (the problem is NP-hard), but we see that the greedy algorithm does pretty well, and there is some evidence that it does even better for primitive groups.

Proof The first part of the theorem is easy to prove: if G has a base of size b then $|G| \leq n^b$, as we remarked earlier; if an irredundent base has size b', then $|G| \geq 2^{b'}$.

The second part is proved by an elementary but ingenious argument of Kenneth Blaha.Let G be a permutation group of degree n with base size b. For any subgroup H of G, there is a b-tuple whose stabiliser in H is the identity; so H has an orbit of length $|H|$ on Ω^b, and hence an orbit of length at least $|H|^{1/b}$ on Ω. So, with H_i the stabiliser of the first i base points found by the greedy algorithm, we see that $|H_i : H_{i+1}| \geq n^{1/b}$, or $|H_{i+1}| \leq |H|^{1-1/b}$.

By induction,

$$|H_i| \leq n^{(1-1/b)^i}$$

for all i. Taking $i = b\log\log n$, we get

$$|H_i| \leq n^{(1-1/b)^{b\log\log n}} \leq n^{b\mathrm{e}^{-\log\log n}} = n^{b/\log n} = \mathrm{e}^b,$$

and a further $b\log_2 \mathrm{e}$ base points chosen in any irredundant way take us to the identity. □

Tim Burness and co-authors proved the following theorem about almost simple primitive groups, see [11]:

Theorem 2.9 (uses CFSG) *Let G be an almost simple primitive permutation group. Then one of the following holds:*

(a) G is a symmetric or alternating group S_m or A_m, acting on the set of k-element subsets of $\{1,\ldots,m\}$, for some k,m;

(b) G is a classical group, acting on an orbit of subspaces, or complementary pairs of subspaces, in its natural module;

(c) the minimal base size for G is at most 7.

In the last case, equality holds only in the case $G = M_{24}$.

It is worth noting here that Babai [9] (for primitive groups which are not 2-transitive) and Pyber [27] (for 2-transitive groups) have given "elementary" proofs (not using CFSG) of results a little weaker than this, but adequate for some purposes. Babai's argument, purely combinatorial, involves finding a bound for the base size in a primitive (but not 2-transitive) group, and then using the fact that a permutation group of degree n with a base of size b has order at most n^b.

CHAPTER 3

Synchronization

The notion of synchronization arises in automata theory, but has very close links with transformation semigroups. The concept has had a lot of attention, partly because of the *Černý conjecture*; we begin with an account of this very addictive conjecture. See [30] for more.

3.1 The dungeon

You are in a dungeon consisting of a number of rooms. Passages are marked with coloured arrows. Each room contains a special door; in one room, the door leads to freedom, but in all the others, to instant death. You have a schematic map of the dungeon (Figure 3.1), but you do not know where you are.

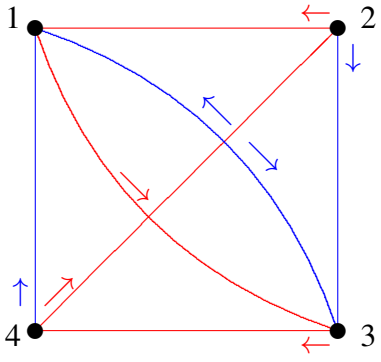


Figure 3.1: The dungeon

You can check that (Blue, Red, Blue) takes you to room 1 no matter where

you start.

What Figure 3.1 shows is a finite-state deterministic *automaton*. This is a machine with a finite set of *states*, and a finite set of *transitions*, each transition being a map from the set of states to itself. The machine starts in an arbitrary state, and reads a word over an alphabet consisting of labels for the transitions (Red and Blue in the example); each time it reads a letter, it undergoes the corresponding transition.

Our automata are particularly simple. There is no distinguished start state, no "accept state", no regular language, no nondeterminism.

A *reset word* is a word with the property that, if the automaton reads this word, it arrives at the same state, independent of its start state. An automaton which possesses a reset word is called *synchronizing*.

Not every finite automaton has a reset word. For example, if every transition is a permutation, then every word in the transitions evaluates to a permutation. How do we recognise when an automaton is synchronizing?

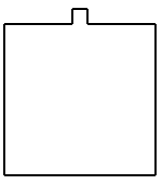
3.2 Synchronization

Combinatorially, an automaton is an edge-coloured digraph with one edge of each colour out of each vertex. Vertices are states, colours are transitions.

Algebraically, if $\Omega = \{1, \ldots, n\}$ is the set of states, then any transition is a map from Ω to itself. Reading a word composes the corresponding maps, so the set of maps corresponding to all words is a transformation semigroup (indeed, a transformation monoid) on Ω.

The notion of synchronization arises in industrial robotics. Parts are delivered by conveyor belt to a robot which is assembling something. Each part must be put on in the correct orientation. One way to do this would be to equip the robot with sensors, information processing, and manipulators. An easier way involves synchronization.

Let us, for a simple case, suppose that the pieces are square, with a small projection on one side:



Suppose the conveyor has a square tray in which the pieces can lie in any orientation. Simple gadgets can be devised so that the first gadget rotates the square through 90° anticlockwise; the second rotates it only if it detects that the projec-

tion is pointing towards the top. The set-up can be represented by an automaton with four states and two transitions, as in Figure 3.2.

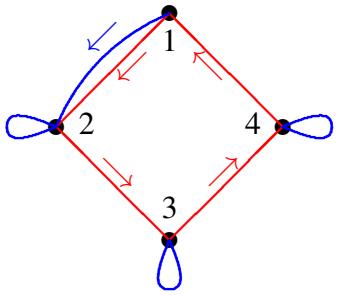


Figure 3.2: An industrial automaton

Now it can be verified that BRRRBRRRB is a reset word (and indeed that it is the shortest possible reset word for this automaton).

This is a special case of the *Černý conjecture*, made about fifty years ago and still open:

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

The above example and the obvious generalisation show that the conjecture, if true, is best possible.

The Černý conjecture has been proved in some cases, but the best general upper bound known is $O(n^3)$, due to Pin. Here is a proof of an $O(n^3)$ bound, which does not get the best constant, but illustrates a simple but important principle.

Proposition 3.1 *An automaton is synchronizing if and only if, for any two states a, b, there is a word in the transitions which takes the automaton to the same place starting from either a or b.*

Proof The forward implication is clear. So suppose the condition of the Proposition holds. Choose an element f of the monoid generated by the transitions which has smallest possible rank. If this rank is greater than 1, choose two points a and b in the image. By assumption, there is an element h which maps a and b to the same place; so the rank of fh is less than the rank of f, a contradiction. □

Now to obtain our bound, consider the diagram of the automaton extended to include pairs of states (shown for our industrial example in Figure 3.3).

According to the lemma, we only have to check whether there is a path from each vertex on the right (a pair of states) to a vertex on the left (a single state).

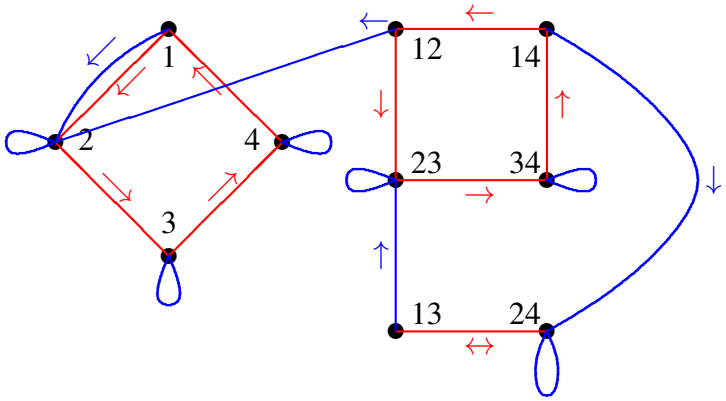


Figure 3.3: An extended diagram of an automaton

The length of such a path is $O(n^2)$, and questions of connectedness can easily be checked. We only have to take such paths at most $n-1$ times. Moreover, checking this can be done in polynomial time, so we can test efficiently for the synchronization property. However, it is known that finding the shortest reset word is NP-hard.

3.3 Graph endomorphisms

We now take a little detour to discuss graph endomorphisms. A *graph* has vertices and edges, each edge joining two vertices; we assume that the edge has no direction (no initial or terminal vertex). An edge is a *loop* if the two vertices are equal, a *link* otherwise. Two edges are *parallel* if they join the same two vertices. A graph is *simple* if it has no loops and no two parallel edges.

Let Γ and Δ be simple undirected graphs. A homomorphism from Γ to Δ should be a structure-preserving map. Since the structure of a graph is given by its edges, we make the definition as follows.

A *homomorphism* from graph Γ to graph Δ is a map f from the vertex set of Γ to that of Δ with the property that, for any edge $\{v,w\}$ of Γ, the image $\{vf,wf\}$ is an edge of Δ.

Parallel edges make no difference to this concept. However, the existence of loops changes things enormously. In a loopless graph, the images of adjacent vertices must be distinct; but, if Δ had a loop on a vertex x, we could map the whole of Γ to x. Similarly, the existence of directions on the edges makes a difference. For us, graphs will always be simple.

The book by Hell and Nešetřil contains much more on graph homomorphisms.

Let K_n be a complete graph on n vertices: all pairs of vertices are joined by edges. Also, let $\omega(\Gamma)$ denote the *clique number* of Γ, the size of the largest complete subgraph of Γ; and let $\chi(\Gamma)$ be the *chromatic number* of Γ, the minimum

number of colours required to colour the vertices so that adjacent vertices receive different colours (this is called a *proper colouring* of Γ).

Proposition 3.2 *(a) A homomorphism from K_n to Γ is an embedding of K_n into Γ; such a homomorphism exists if and only if $\omega(\Gamma) \geq n$.*

(b) A homomorphism from Γ to K_n is a proper colouring of Γ with n colours; such a homomorphism exists if and only if $\chi(\Gamma) \leq n$.

(c) There are homomorphisms in both directions between Γ and K_n if and only if $\omega(\Gamma) = \chi(\Gamma) = n$.

An *endomorphism* of a graph Γ is a homomorphism from Γ to itself, and an *automorphism* is a bijective endomorphism. The set of all endomorphisms of a graph is a transformation monoid on the vertex set of the graph, and the set of automorphisms is a permutation group. [**Caution:** This definition of automorphism fails in the infinite case, where we must also assume that the inverse map is an endomorphism.]

3.4 Endomorphisms and synchronization

The single obstruction to a semigroup S being synchronizing is the existence of a graph Γ such that $S \leq \mathrm{End}(\Gamma)$, as we now show.

Theorem 3.3 *Let S be a transformation monoid on Ω. Then S fails to be synchronizing if and only if there exists a non-null graph Γ on the vertex set Ω for which $S \leq \mathrm{End}(\Gamma)$. Moreover, we may assume that $\omega(\Gamma) = \chi(\Gamma)$.*

Proof Since endomorphisms cannot collapse edges to single vertices, if Γ is non-null and $S \leq \mathrm{End}(\Gamma)$, then clearly S is non-synchronizing.

For the converse, we have to build a graph from a transformation semigroup. The construction is as follows. Given a transformation semigroup S on Ω, the graph $\mathrm{Gr}(S)$ is defined to have vertex set Ω, and edges all pairs $\{v,w\}$ for which there does not exist an element $s \in S$ satisfying $vs = ws$. We show

(a) $S \leq \mathrm{End}(\Gamma)$;

(b) $\omega(\Gamma) = \chi(\Gamma)$;

(c) Γ is non-null if and only if S is non-synchronizing.

Proof of (a): Let $\{v,w\}$ be an edge of Γ and $s \in S$; we have to show that $\{vs,ws\}$ is an edge. The other possibilities are:

- $vs = ws$: this contradicts the definition of Γ.
- $\{vs,ws\}$ is a non-edge: then there exists $t \in S$ with

$$v(st) = (vs)t = (ws)t = w(st),$$

and so $\{v,w\}$ is a non-edge, contrary to assumption.

Proof of (b): Choose an element $s \in S$ of minimum rank; let $K = \mathrm{Ker}(S)$ and $A = \mathrm{Im}(S)$.

Then A is a clique. For if $v,w \in A$ are not joined by an edge, then there exists $t \in S$ with $vt = wt$; so $|\mathrm{Im}(st)| < |\mathrm{Im}(s)|$, a contradiction.

Also, P is a partition into independent sets. For two points in the same part of P are mapped to the same point by s, so by definition are not joined.

Thus

$$\chi(\mathrm{Gr}(S)) \leq r \leq \omega(\mathrm{Gr}(S)) \leq \chi(\mathrm{Gr}(S)),$$

the last inequality holding in any graph; so we have equality.

Proof of (c): If $\mathrm{Gr}(S)$ is non-null, then (a) shows that S is not synchronizing. Conversely, if $\mathrm{Gr}(S)$ is null, then any pair of points can be collapsed by an element of S; Proposition 3.1 shows that S is synchronizing. □

3.5 Synchronizing groups

The best reference for the remainder of this chapter is [8].

A permutation group is never synchronizing as a monoid, since no collapses at all occur.

We abuse language by making the following definition. A permutation group G on Ω is *synchronizing* if, for any map f on Ω which is not a permutation, the monoid $\langle G, f\rangle$ generated by G and f is synchronizing.

From our characterisation of synchronizing monoids, we obtain the following.

Theorem 3.4 *A permutation group G on Ω is non-synchronizing if and only if there exists a G-invariant graph Γ, not complete or null, which has clique number equal to chromatic number.*

Proof Suppose that such a graph Γ exists. Then

$$G \leq \mathrm{Aut}(\Gamma) \leq \mathrm{End}(\Gamma),$$

and $\mathrm{End}(\Gamma)$ is a non-synchronizing monoid. Let f be an element of $\mathrm{End}(\Gamma)$ which is not a permutation. (For example, choose a clique A of size r, and an r-colouring c of Γ; let f map the ith colour class of c to the ith vertex in A.) Then $\langle G, f\rangle \leq \mathrm{End}(\Gamma)$, so this monoid is not synchronizing.

Conversely, suppose that f is a map such that $\langle G, f\rangle$ is a non-synchronizing monoid. By Theorem 3.3, there is a graph Γ with clique number equal to chromatic number, such that $\langle G, f\rangle \leq \mathrm{End}(\Gamma)$; in particular, $G \leq \mathrm{Aut}(\Gamma)$. □

Corollary 3.5 *Let G be a permutation group of degree $n > 2$.*

(a) If G is synchronizing, then it is transitive, primitive, and basic.

(b) If G is 2-homogeneous, then it is synchronizing.

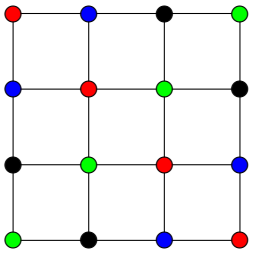
Proof (a) If G is intransitive, let Γ be the complete graph on a non-singleton G-orbit (or, if all G-orbits are singletons, the union of two of them), with no further edges. Then Γ has clique and chromatic number equal to the size of this complete graph.

If G is imprimitive, let Γ be the complete multipartite graph whose parts are the parts of a nontrivial G-invariant partition. Then Γ has clique number and chromatic number equal to the number of parts of the partition.

Suppose that G is non-basic, and let G preserve the Cartesian structure A^n. Form a graph (the *Hamming graph*) in which two vertices are joined if the n-tuples differ in just a single place. Clearly $G \leq \mathrm{Aut}(\Gamma)$. Now the clique number of Γ is at least $|A|$, since the set of n-tuples with fixed entries in all but the first coordinate is a clique of size $|A|$. Also, the chromatic number of Γ is at most $|A|$, since we can give a $|A|$-colouring as follows: Identify A with an abelian group of order $|A|$ (for example, the cyclic group), and choose the set of colours also to be A. Now give the n-tuple $(a_1, \ldots, a_n)$ the colour $a_1 + \cdots + a_n$. If two vertices are adjacent, they agree in all but one coordinate, and so they get different colours; so this is a proper colouring. It follows that $\omega(\Gamma) = \chi(\Gamma) = |A|$.

(b) If G is 2-homogeneous, then the only G-invariant graphs are the complete and null graphs. □

In the case of 2-dimensional Hamming graphs, a colouring with $|A|$ colours can be identified with a Latin square. This example uses the Klein group:



In higher dimensions, such colourings correspond to more complicated combinatorial objects.

So synchronizing groups form an interesting class lying between basic primitive groups and 2-homogeneous groups. We give an example to show that the containments are strict.

Example Let G be the group induced by S_n on the set of 2-element subsets of $\{1,\ldots,n\}$. Then G is primitive for $n > 4$. (For $n = 4$, the relation "equal or disjoint" is a G-invariant equivalence relation on 2-sets.) It is clearly basic, and not 2-homogeneous for $n > 3$.

We show that G is synchronizing if and only if n is odd. We may assume that $n \geq 5$.

There are two G-invariant graphs: the graph where two pairs are joined if they intersect (aka the *triangular graph* $T(n)$, or the line graph of K_n) and the graph where two pairs are joined if they are disjoint (the *Kneser graph* $K(n,2)$).

- The triangular graph has clique number $n-1$, a maximum clique consisting of all pairs containing one given point of the n-set. Its chromatic number is the *chromatic index* or edge-chromatic number) of K_n, which is well known to be $n-1$ if n is even, or n if n is odd. (Indeed, if n is odd, a set of pairwise disjoint pairs has size at most $(n-1)/2$, so the chromatic number is at least n.)
- The clique number of the Kneser graph is $n/2$ if n is even, and $(n-1)/2$ if n is odd (by the argument just given). It is elementary to see that the chromatic number is strictly larger; in fact, a celebrated theorem of Lovász shows that the chromatic number is $n-2$.

So our claim follows.

3.6 Separating groups

First, a brief word about complexity questions for permutation groups.

A permutation group on a set of n elements can be specified by a set of generators. It is known that such a group can be generated by at most $n/2$ elements if $n > 3$; so "polynomial in the input size" should be the same as "polynomial in n". There is a problem with this: your opponent is not constrained to give you a generating set of minimal size, but could simply add huge numbers of redundant elements to the input. This is unavoidable; but there are algorithms which get around the problem to some extent. For example, a filter developed by Mark Jerrum does the following. Permutations are given one at a time; after receiving

each permutation, it is possible to do a polynomial-time computation which results in a set of at most $n-1$ permutations which generate the same group as all the permutations received so far.

So we ignore the problem and simply assume that any group we consider is generated by at most $n-1$ permutations.

There are easy polynomial-time algorithms for computing orbits, and hence transitivity, and also t-homogeneity and t-transitivity (for fixed t). (An orbit is a connected component of the union of the functional digraphs corresponding to the generators.) Moreover, there is a polynomial-time algorithm which tests primitivity, and returns a system of minimal blocks of imprimitivity if one exists.

By contrast, we have the following stupid-looking algorithm to test whether G is synchronizing:

(a) Compute the orbits of G on 2-sets. Suppose there are r of these; then there are 2^r-2 non-trivial G-invariant graphs.

(b) For each such graph, test whether its clique number is equal to its chromatic number. If this ever happens, the group is not synchronizing; otherwise it is synchronizing.

The obvious problems are that there are potentially exponentially many graphs to check (though for many interesting primitive groups, the number r is quite small), and that clique number and chromatic number are NP-hard. Nevertheless, this algorithm has been implemented and used to test groups with degrees well into the hundreds.

It is possible to make a small improvement. The motivation is an idea from parameterised complexity theory, which justifies saying that, though the two problems mentioned are NP-hard, clique number is in some sense easier than chromatic number. (In practice this is certainly true: the GAP package `Grape` finds the clique number of a graph with large automorphism group very efficiently, while chromatic number tests are much slower.)

The basic result is the following.

Proposition 3.6 *Let G be a transitive permutation group on Ω. Suppose that A and B are subsets of Ω with the property that, for all $g \in G$, we have $|Ag \cap B| \leq 1$. Then $|A| \cdot |B| \leq |\Omega|$.*

Proof Count triples (a,b,g) with $a \in A$, $b \in B$, $g \in G$, and $ag = b$.

On the one hand, there are $|A|$ choices of a and $|B|$ choices of b; then the set of elements of G mapping a to b is a coset of the stabiliser of a, and so there are $|G|/|\Omega|$ such elements, by the Orbit-Stabiliser Theorem. So the number of triples is $|A| \cdot |B| \cdot |G|/|\Omega|$.

On the other hand, for each $g \in G$, we have $|Ag \cap B| \leq 1$, so there is at most one choice of a and b. So there are at most $|G|$ such triples.

The result follows. □

The argument shows that, if equality holds, then $|Ag \cap B| = 1$ for all $g \in G$.

Note that the hypothesis of the proposition is satisfied if A is a clique and B an independent set in a vertex-transitive graph. Let $\alpha(\Gamma)$ be the *independence number* of Γ (the size of the largest independent set of Γ, in other words, the clique number of the complementary graph. Then we have:

Corollary 3.7 *If Γ is a vertex-transitive graph on n vertices, then*

$$\omega(\Gamma) \cdot \alpha(\Gamma) \leq n.$$

We say that a transitive permutation group G on a set Ω is *separating* if, given any two subsets A and B of Ω with $|A| \cdot |B| = |\Omega|$ and $|A|, |B| > 1$, there exists $g \in G$ such that $Ag \cap B = \emptyset$: in other words, A and B can be "separated" by an element of G.

The argument in the previous proposition shows that, if sets A and B witness that G is non-separating, then $|Ag \cap B| = 1$ for all $g \in G$.

Proposition 3.8 *A separating group is synchronizing.*

Proof If G is non-synchronizing, let P be a partition of Ω and A a G-section for P; let B be a part of P. Then $|A| \cdot |B| = |\Omega|$ and $|Ag \cap B| = 1$ for all $g \in G$. □

Theorem 3.9 *The transitive group G on Ω is non-separating if and only if there exists a G-invariant graph Γ on Ω, not complete or null, such that*

$$\omega(\Gamma) \cdot \alpha(\Gamma) = |\Omega|.$$

Proof If such a graph Γ exists, we can take A and B to be a clique and an independent set of maximum size in Γ to witness non-separation.

Conversely, suppose that G is non-separating, and let A and B be sets witnessing this property. No element of G can map a 2-subset of A to a 2-subset of B. So form a graph whose edges are the images under G of the 2-subsets of A; the graph is G-invariant, and A is a clique and B an independent set. Since the product of their cardinalities is $|\Omega|$, they are both of maximum size. □

So we can modify the test for synchronization as follows:

(a) Compute the orbits of G on 2-sets. Suppose there are r of these; then there are $2^r - 2$ non-trivial G-invariant graphs, falling into $2^{r-1} - 1$ complementary pairs.

(b) For each such pair, find the clique numbers of the two graphs, and test whether their product is n. If this ever happens, the group is not separating, and we have to find the chromatic numbers of both graphs to test whether it is synchronizing or not; otherwise it is separating, and hence synchronizing.

If it were the case that "synchronizing" and "separating" were equivalent, then the step involving finding chromatic number could be omitted, and the algorithm would only need to find clique numbers of graphs. This is not so, but one has to look quite far to find an example of a group which is synchronizing but not separating.

Such an example can be found as follows.

Let V be a 5-dimensional vector space over a finite field F of odd characteristic, and Q a non-singular quadratic form on V. It can be shown that there is a choice of basis such that, in coordinates,

$$Q(x_1,\ldots,x_5) = x_1x_2 + x_3x_4 + x_5^2.$$

The *quadric* associated with Q is the set of points in the projective space based on V (that is, 1-dimensional subspaces of V) on which Q vanishes. It can be shown that the number of points on the quadric is $(q+1)(q^2+1)$. The associated orthogonal group $O_5(F)$ acts on the quadric; it is transitive on the points, and has just two orbits on pairs of points, corresponding to orthogonality and non-orthogonality with respect to the associated bilinear form.

Let Γ be the graph in which two points are joined if they are orthogonal. Then it is known that

- the clique number of Γ is $(q+1)$, and the cliques of maximal size are *totally singular lines* on the quadric (the point sets of 2-dimensional subspaces on which the form vanishes identically – the span of the first and third basis vectors is an example);
- the independence number of Γ is q^2+1, and the independent sets of maximal size are *ovoids* of the quadric, sets of points meeting every line in exactly one point.

We see from this that $O_5(q)$ is not separating. Is it synchronizing?

A colouring of the complement of Γ with q^2+1 colours would be a *spread*, a partition of the quadric into totally singular lines; it is a standard fact that no such partition can exist. A colouring of Γ with $q+1$ colours, on the other hand, is a partition of the quadric into $q+1$ ovoids. Now, for $|F| = 3$, 5, or 7, it has been proved that the only ovoids on this quadric are hyperplane sections (quadrics in 3-dimensional projective space). Any two hyperplanes intersect in a plane, and the corresponding quadrics meet in a conic in the plane; so there are no two disjoint

ovoids, and *a fortiori* no partitions into ovoids, in this case. So we have three examples of groups which are synchronizing but not separating. (The classification of ovoids over larger fields is unknown.)

Note how this simple question in synchronization theory leads to the frontiers of knowledge in finite geometry! For further information about the geometry involved in this example, see the books by Hirschfeld and Thas (the last chapter concerns ovoids and spreads) and, for the groups, by Taylor.

3.7 Almost synchronizing groups

The material in this section is taken from [4].

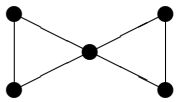
As we have seen, if the transitive group G fails to be synchronizing, then there is a G-invariant graph Γ with $\omega(\Gamma) = \chi(\Gamma) = r$, say. All the colour classes in the colouring have the same size n/r. Thus, the maps of minimum rank not synchronized by a transitive group are *uniform*, meaning that all kernel classes have the same size.

We say that a transitive group is *almost synchronizing* if it synchronizes all non-uniform maps. An almost synchronizing group is primitive (since an imprimitive group preserves a complete multipartite graph, which has many non-uniform endomorphisms). It was thought for a time that the converse might be true. This hope was encouraged by results like the following:

Proposition 3.10 *A primitive group of degree n synchronizes all maps of rank at most 3, and all maps of rank $n-4$ or greater.*

Indeed, G synchronizes every map of rank $n-1$ if and only if it is primitive.

However, the guess turned out to be wrong. The smallest example is a graph on 45 vertices, the line graph of the *Tutte–Coxeter graph*, the 8-cage on 30 vertices (the incidence graph of the generalized quadrangle of order 2). The Tutte–Coxeter graph has valency 3 and girth 8. It follows that its line graph has valency 4, and the closed neighbourhood of a vertex is the *butterfly*:



The whole graph has a non-uniform endomorphism onto the butterfly, where 15 vertices map to the body, 10 to the vertices on one wing, and 5 to those on the other. Now combining this with the butterfly folding its wings together, we get a uniform endomorphism of rank 3 onto a triangle (a 3-colouring of the graph). Indeed, this graph also has endomorphisms of rank 7 as well (the image consisting of three triangles).

Several other examples are known, but there is no general theory of such things.

CHAPTER 4

Regularity and idempotent generation

Our aim in this section is to consider classes of transformation semigroups $S \leq T_n$, and investigate properties such as regularity and idempotent generation. There is a permutation group associated with S in one of two possible ways: either S contains permutations, in which case $S \cap S_n$ is a permutation group; or the *normaliser* of S in the symmetric group, the set

$$\{g \in S_n : (\forall s \in S) g^{-1} s g \in S\}$$

is a permutation group. In either case, as we will see, the group G influences the structure of S.

Much as in the last chapter, we look first at semigroups of the form $\langle G, f \rangle$, where $G \leq S_n$ and $f \in T_n \setminus S_n$. If we can understand these semigroups, then we can proceed to add two or more non-permutations.

4.1 Regularity

The material in this section is from [5].

Both regularity and idempotent generation are connected with an observation we made earlier. Suppose that G is a permutation group, f a transformation, and $fg_1fg_2f\cdots g_rf = f$. Then, for each i, fg_if has the same rank as f. This implies that g_i must map the image of f to a section (transversal) for the kernel of f.

Which permutation groups G have the property that, for any map f of rank k, the element f is regular in $\langle G, f \rangle$? Since the kernel and image of such a map f are an arbitrary k-partition and an arbitrary k-subset, we see that a necessary condition is that G has the following *k-universal transversal property*:

> For any k-set A and any k-partition P, there is an element $g \in G$ such that Ag is a transversal for P.

So the first question we have to consider is the classification of groups with the k-universal transversal property (or k-ut property, for short).

It turns out that this property has much stronger consequences. The implication we saw above reverses, and more besides:

Theorem 4.1 *Given k with $1 \leq k \leq n/2$, the following conditions are equivalent for a subgroup G of S_n:*

(a) For any rank k map f, f is regular in $\langle G, f\rangle$.

(b) For any rank k map f, $\langle G, f\rangle$ is regular (this means that all its elements are regular).

(c) For any rank k map f, f is regular in $\langle g^{-1}fg : g \in G\rangle$.

(d) For any rank k map f, $\langle g^{-1}fg : g \in G\rangle$ is regular.

(e) G has the k-universal transversal property.

The equivalence of (a) and (c) has been known for some time; but the equivalence of these two conditions with (b) and (d) is a bit of a surprise. The semigroup $\langle G, f\rangle$ usually contains elements with rank smaller than k; in order to show that these are regular, we need to know that G has the l-universal transversal property, for all $l < k$:

Theorem 4.2 *For $2 \leq k \leq n/2$, the k-ut property implies the $(k-1)$-ut property.*

This is reminiscent of part of the Livingstone–Wagner theorem that we saw in the second chapter. The first result in their paper was a proof that, for $k \leq n/2$, a k-homogeneous permutation group is $(k-1)$-homogeneous. Their proof used some simple facts about the character theory of the symmetric group: if you are familiar with the theory, here are the steps:

(a) The number of orbits of a permutation group G is the multiplicity of the trivial character in the permutation character.

(b) Hence, if G has two actions such that the permutation character of the first is contained in the permutation character of the second, then the number of orbits in the second action is at least as great as the number in the first action.

(c) The permutation character $\pi^{(k,n-k)}$ of the symmetric group S_n on k-sets, for $k \leq n/2$, satisfies $\pi^{(k-1,n-k+1)} \subseteq \pi^{(k,n-k)}$, since

$$\pi^{(n-k,k)} = \sum_{i=0}^{k} \chi^{(n-i,i)}.$$

However, the argument can be made entirely combinatorial, as was done by Kantor. If a permutation group G acts on the rows and columns of a matrix A with rank r so as to preserve the matrix A, then the two actions have a common constituent of degree r. In particular, if the rank of A is equal to the number of rows, then the permutation character on rows is contained in the character on columns. To prove (c) above, we take the incidence matrix of $(k-1)$-sets and k-sets (where incidence is inclusion): a purely combinatorial argument shows that its rank is $\binom{n}{k-1}$ if $k \leq n/2$.

However, there seems to be no purely combinatorial proof that the k-ut property implies the $(k-1)$-ut property for $k \leq n/2$. So we have to make a long detour, which comes close to giving a complete classification of these groups for $k > 2$.

Which permutation groups have the k-ut property? In one case, the answer is simple (but shows that there is no hope of a classification):

Proposition 4.3 *A permutation group has the 2-ut property if and only if it is primitive.*

Proof Given a 2-set A, the G-orbit of A is the set of edges of a minimal non-null G-invariant graph. To say that the edge set of a graph contains a transversal to every 2-partition is just to say that the graph is connected. So 2-ut is equivalent to the assertion that every non-null G-invariant graph is connected; this property is equivalent to primitivity, as we saw in Proposition 2.5. □

For larger values of k, we begin to get some hold on the group. Let us say that, if $l \leq k$, a permutation group G is (l,k)-*homogeneous* if, for any l-set A and k-set B, there exists $g \in G$ with $Ag \subseteq B$. If $l = k$, this is just k-homogeneity as previously defined.

Now observe that

If G has the k-ut, then G is $(k-1,k)$-homogeneous.

For, given A and B as in the definition, take the k-partition P which has the elements of A as singleton parts and one part including everything else; then a k-set is a transversal for P if and only it contains A. So, if G has k-ut, there exists B such that $Bg \supseteq A$; now the inverse of g satisfies $Ag^{-1} \subseteq B$.

Also, there is a close connection between $(k-1,k)$-homogeneity and $(k-1)$-homogeneity. Certainly the second of these properties implies the first. In addition, we have

> There is a function f such that, if G is $(k-1,k)$-homogeneous of degree $n \geq f(k)$, then G is $(k-1)$-homogeneous.

For this, we take $f(k)$ to be the Ramsey number $R_{k-1}(k,k)$. Suppose that $n \geq R_{k-1}(k,k)$ and G is not $(k-1)$-homogeneous; colour the $(k-1)$-sets in one orbit red, and the remaining ones blue. The inequality on n implies that there is a monochromatic k-set; if it is red, then no blue $(k-1)$-set can be mapped inside it by G, and *vice versa*.

Now the analysis involves showing that, with just five exceptions (with degrees 5, 7 and 9), a $(k-1,k)$ homogeneous group of degree n, with $k \leq n/2$, is $(k-1)$-homogeneous. The proof involves showing, by mostly combinatorial arguments, that such a group must be 2-transitive, and then invoking the classification of the 2-transitive groups (a consequence of CFSG). Now Theorem 4.2 follows from this, since a $(k-1)$-homogeneous group obviously has the $(k-1)$-ut property.

The permutation groups which are $(k-1,k)$-homogeneous, and those with the k-universal transversal property, have been almost completely classified; a few stubborn families of groups (including the Suzuki groups for $k = 3$) are still holding out.

The ultimate problem in this line of research would be a classification of all pairs (G,f), where G is a permutation group and f a non-permutation on $\{1,\ldots,n\}$, such that f is regular in $\langle G,f\rangle$ (or indeed, such that another of the first four conditions of Theorem 4.1 holds – these conditions are not all equivalent at this level of generality).

We are a long way from such a result, but there are already some partial results on the following question:

> Given k with $1 \leq k \leq n/2$, for which permutation groups G of degree n and k-subsets A of the domain is it the case that, for all maps f with $\mathrm{Im}(f) = A$, the element f is regular in $\langle G,f\rangle$?

For this problem, where we fix the image rather than asking about all maps with image of size k, a weaker property than the k-ut is required. We say that G has the *k-existential transversal property*, or k-et property for short, if there exists a k-subset A such that, for any k-partition P, there is an element $g \in G$ such that Ag is a transversal for P. We call A a *witnessing st* for the k-et property.

Work has begun on groups with the k-et property. It is hampered by the fact that we do not know whether k-et implies $(k-1)$-et for $1 < k \leq n/2$. Also, the connection with homogeneity is not so straightforward. For example, the Mathieu group M_{24} (which is 5-transitive but not more) has the 7-et property.

However, using CFSG and quite a bit of effort, it has been possible to show:

Theorem 4.4 *Suppose that $8 \leq k \leq n/2$. Then a transitive permutation group of degree n with the k-et property is the symmetric or alternating group.*

The example M_{24} shows that 8 is best possible in this theorem; but probably M_{24} is the only further example for the 7-et property.

Here is a short account of the proof, giving the main techniques used.

Suppose that G has the k-et property and let A be a witnessing set. First note that A contains a representative of every G-orbit on $(k-1)$-sets. For, if B is a $(k-1)$-set, let P be the partition which has the singletons of B as parts and a single part containing everything else. Then A can be mapped to a transversal for P, that is, a k-set containing B.

In particular, this means that G has at most k-orbits on $(k-1)$-sets, and so

$$|G| \geq \binom{n}{k-1} \Big/ k.$$

We call this the *order bound*, and return to it shortly. We note that the right-hand side of the order bound gets stronger as k increases (for $k \leq n/2$); so, if G fails the bound for some k, then it fails for all larger k.

The other main technique is that, if G is a group of automorphisms of some combinatorial structure, we can often find two $(k-1)$-subsets of that structure which cannot "coexist" inside a k-set, which would contradict the above property of the witnessing k-set. For example, suppose that $k = 4$, and that G is imprimitive, with at least three blocks each of size at least 3. Then a 3-subset of a block and a 3-set containing a point from each of three distinct blocks cannot coexist. Pursuing this argument a little further, we conclude that, for $k \geq 4$, G must be primitive.

Confronting the order bound with either Maróti's bound, or the bound derived from the base size bound of Burness *et al.* (see Theorems 2.7 and 2.9) leaves a relatively small number of types of primitive group to be considered; the technique then is to examine the structures these groups act on, and find pairs of $(k-1)$-sets which cannot coexist.

For example, suppose that G is one of the "large" primitive groups, S_m or A_m, in its action on 2-sets. As we saw in the preceding chapter, G preserves a graph (the line graph of K_m) which contains a clique of size $m-1$ and an independent set of size $\lfloor m/2 \rfloor$, which cannot coexist inside a set of size less than $m-2+\lfloor m/2 \rfloor$; so k must be at least this value. Now it is easy to see that there are more than k orbits on $(k-1)$-sets (these orbits correspond to graphs with $k-1$ edges).

4.2 Idempotent generation

The material in this section is from [6].

It turns out that some of the same considerations are required for studying idempotent-generation. Note first that a non-identity permutation is never generated by idempotents, so we should ask only for $\langle G, f\rangle \setminus G$ to be idempotent-generated.

There is a connection between idempotents and k-et. This is a slight variant of the argument we saw in Proposition 1.9.

Proposition 4.5 *Suppose that G is a permutation group. Then $\langle G, f\rangle$ contains an idempotent of rank k for any map f of rank k if and only if G has the k-universal transversal property.*

Proof Suppose that G has the k-ut property. Let f be a map of rank k, with kernel P and image A. Choose g such that Ag is a transversal to P. Then fg maps Ag to itself; and so some power of fg acts as the identity on Ag, and is an idempotent of rank k.

Conversely, let A be a k-set and P a k-partition. Choose a map f with kernel P and image A. By assumption, $\langle G, f\rangle$ contains an idempotent e of rank k; without loss, $e = fg_1fg_2\cdots fg_r$. (If the expression for e begins with an element of g, conjugate by this element to move it to the end.) Now the rank of fg_1 is equal to k, and so Ag_1 is a transversal to P, as required. □

However, for $\langle G, f\rangle \setminus G$ to be idempotent-generated for all rank k maps f is a stronger condition. First note that the condition is empty for $k = 1$, since every rank 1 map is an idempotent; so $k = 2$ is the first non-trivial case.

In general, a combinatorial equivalent to idempotent generation is not known. (There is a condition, the *strong k-ut property*, which implies idempotent-generation, but is not equivalent to it.) There is such a condition in the case $k = 2$, leading to an interesting open problem in permutation groups. Recall first that the 2-ut property is equivalent to primitivity, so whatever our condition is, it must be stronger than primitivity.

Let G be a primitive permutation group on Ω. As suggested earlier, we are interested in *orbital graphs* for G: these are the graphs with vertex set Ω, and edge set a single G-orbit on 2-sets. Thus G acts vertex-transitively and edge-transitively on an orbital graph.

We say that G has the *road closure property* if the following holds: for any orbit O of G on 2-sets, and any proper block of imprimitivity (smaller than O) for the action of G on O, the graph with vertex set Ω and edge set $O \setminus B$ (obtained by deleting the edges in B from the orbital graph) is connected.

Imagine that the graph represents a connected road network; we ask that, if workmen come along and dig up a proper block of imprimitivity for G, the graph remains connected.

An example of a primitive group which fails to have the road closure property is the automorphism group of the square grid graph (the line graph of $K_{m,m}$: this is primitive for $m > 3$ (but of course not basic, since the grid is a Cartesian structure). See Figure 4.1.

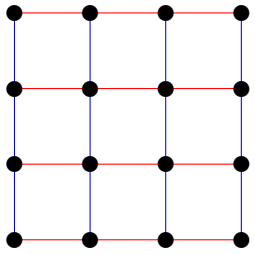


Figure 4.1: A grid

The automorphism group is transitive on the edges of this graph, and has two blocks of imprimitivity, the horizontal and vertical edges (coloured red and blue in the figure). If it is a road network, and if all the blue edges are closed, the network is disconnected: it is no longer possible to travel between different horizontal layers.

Using similar arguments it is possible to show that a primitive group which has the road closure property must be basic.

Here is an example of a basic primitive group which does have the road closure property. The group is $G = S_5$ acting on 2-sets; one orbital graph for it is the *Petersen graph* (Figure 4.2). Now the group G acts transitively on the 15 edges, which fall into five groups of three mutually parallel or perpendicular edges in the standard drawing of the graph, as shown in the figure; these triples are the maximal blocks of imprimitivity. It is clear that, when the three edges shown in red are removed, the graph remains connected.

And here is a basic group which fails the road closure property. We take G to be the group of automorphisms and dualities (maps which interchange points and lines but preserve incidence) of the *Fano plane* (Figure 4.3). G acts on the *flags* of the Fano plane; the action is primitive. We consider the orbital graph in which two flags are joined if they share a point or a line. The edges fall into two types which are blocks of imprimitivity, depending on whether the two flags share a point or a line. If we remove the edges joining flags sharing a point, then from a given flag we can only move to the other two flags using the same line; so the graph is disconnected.

The connection with our problem is:

Theorem 4.6 *Let G be a primitive permutation group on Ω. Then the following are equivalent:*

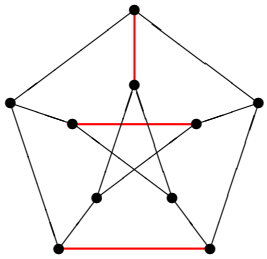


Figure 4.2: The Petersen graph

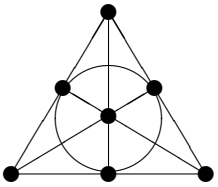


Figure 4.3: The Fano plane

(a) G has the road closure property.

(b) For any rank 2 *map* f, $\langle G, f\rangle \setminus G$ *is idempotent-generated.*

The basic primitive groups which are known to fail the road closure property are rather few, and fall into two classes:

- groups which have an imprimitive normal subgroup of index 2 (the group associated with the Fano plane above is an example);
- a class of groups associated with the triality automorphism of the eight-dimensional orthogonal groups.

It is conjectured that this list is complete. I refer to [6] for further details.

4.3 Partition transitivity and homogeneity

Let f be a map of rank k on Ω, where $|\Omega| = n$, and G a permutation group on Ω, and consider the semigroup $S = \langle G, f\rangle \setminus G$. An element of S of the form

$$s = fg_1fg_2f\cdots fg_rf$$

has the property that $\mathrm{Ker}(s)$ is a coarsening of $\mathrm{Ker}(f)$ (that is, any part of the latter is contained in a part of the former), while $\mathrm{Im}(s)$ is a subset of $\mathrm{Im}(f)$. Pre- and post-multiplying by elements of G, we see that the kernel of any element of S is a G-image of a coarsening of $\mathrm{Ker}(f)$, while the image of any element of S is a G-image of a subset of $\mathrm{Im}(f)$.

If $G = S_n$, then clearly the elements of maxumum rank k in S are all those whose kernels have the same shape as $\mathrm{Ker}(f)$, and whose images have the same cardinality as $\mathrm{Im}(f)$.

Consider the question: Which permutation groups G have the property that

$$\langle G, f\rangle \setminus G = \langle S_n, f\rangle \setminus S_n.$$

Can we classify these groups? We see that this is equivalent to determining groups which are k-homogeneous and λ-homogeneous, where λ is a partition of n with k parts: here, we say that a permutation group G is *λ-homogeneous* if it acts transitively on partitions of Ω of shape λ.

Note that a similar concept, λ-transitive, related to λ-homogeneous much as k-transitive is to k-homogeneous, was introduced by Martin and Sagan [26].

The λ-homogeneous permutation groups were classified in [2], and the problem posed above was solved. The λ-homogeneous groups were independently classified by Dobson and Malnič [16].

A related question concerns groups G for which

$$\langle G, f\rangle \setminus G = \langle g^{-1} f g : g \in G\rangle.$$

Groups for which this property holds for all non-permutations f are called *normalizing groups*, and were determined in [7]: only the symmetric and alternating groups, the trivial group, and finitely many others have this property. The next question in this direction would be to determine the k-normalizing groups, those for which the above two semigroups are equal for all maps of rank k.

4.4 Automorphisms

Perhaps the single most surprising fact about finite groups is the following.

Theorem 4.7 *The only symmetric group (finite or infinite) which admits an outer automorphism is S_6.*

An *outer automorphism* of a group is an automorphism not induced by conjugation by a group element. In the case of symmetric groups, the group elements are all the permutations, and so an outer automorphism is one which is not induced by a permutation.

The outer automorphism of S_6 was known in essence to Sylvester; it arguably lies at the root of constructions taking us to the Mathieu groups M_{12} and M_{24}, the Conway group Co_1, the Fischer–Griess Monster, and the infinite-dimensional Monster Lie algebra. Here is a sketch of Sylvester's construction (in his own idiosyncratic terminology).

Begin with $A = \{1, \ldots, 6\}$, so $|A| = 6$. A *duad* is a 2-element subset of A; so there are 15 duads. A *syntheme* is a set of three duads covering all the elements of A; there are also 15 synthemes. Finally, a *total* (or *synthematic total*) is a set of five synthemes covering all 15 duads. It can be shown that there are 6 totals. Let B be the set of totals.

Then any permutation on A induces permutations on the duads and on the synthemes, and hence on B; this gives a map from the symmetric group on A to the symmetric group on B which is an outer automorphism of S_6.

This outer automorphism has order 2 modulo inner automorphisms. For any syntheme lies in two totals, so we can identify synthemes with duads of totals; any duad lies in three synthemes covering all the totals, so we can identify duads with synthemes of totals; and finally, each element of A lies in 5 duads whose corresponding synthemes of totals form a total of totals!

There are other examples of this phenomenon too. For example, in the second stage of the above process, the Mathieu group M_{12} has an outer automorphism which is not induced by a permutation.

Does anything similar happen for transformation semigroups?

Sullivan [29] proved the following theorem 40 years ago:

Theorem 4.8 *A finite transformation semigroup S containing all the rank* 1 *maps has the property that all its automorphisms are induced by permutations.*

We observe that the rank 1 maps are the minimal idempotents (and so are mapped among themselves by any automorphism), and are naturally in one-to-one correspondence with the points on which the semigroup acts. So what is required is just a proof that only the identity automorphism can fix all the rank 1 maps.

As a corollary, we see:

Corollary 4.9 *Let S be a transformation semigroup which is not a permutation group, whose group of units is a synchronizing permutation group. Then* $\mathrm{Aut}(S)$ *is contained in the symmetric group; that is, all automorphisms of S are induced by conjugation in its normaliser in the symmetric group.*

For, since S contains a synchronizing group G, it contains at least one element of rank 1; and since G is transitive, it contains them all.

And there matters stayed for a long time! But it is tempting to wonder whether we can replace "synchronizing" by "primitive" here.

Recently a small step has been taken. Recall that, if G is not synchronizing, then the smallest possible rank of an element in a non-synchronizing monoid with G as its group of units is 3. The following theorem was shown in [3]:

Theorem 4.10 *Let S be a transformation semigroup containing an element of rank at most* 3*, and whose group of units is a primitive permutation group. Then the above conclusion holds: all automorphisms of S are induced by conjugation in its normaliser in the symmetric group.*

For this, it is necessary to reconstruct the points of Ω from the images and kernels of maps of rank 3 in a way which is invariant under automorphisms of S. This is achieved by counting endomorphisms with various properties. For example, consider the images, which are maximal cliques in a graph Γ with $S \leq \mathrm{End}(\Gamma)$. It is not hard to show that no two such cliques can intersect in two points; we distinguish pairs of cliques intersecting in a point from disjoint pairs of cliques by properties of the idempotents. We refer to the paper for more details.

CHAPTER 5

Other topics

The final chapter covers some connections between semigroups and groups which don't really fit among the earlier material, together with a list of open problems and some basic reading.

5.1 Chains of subsemigroups

The *length* of a group is a useful but not well known measure of its complexity. We define the length $l(G)$ to be the maximal l for which a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_l = \{1\}$$

exists; in other words, one less than the number of subgroups in a maximal chain.

Two simple properties of the length function are:

(a) By Lagrange's Theorem, $l(G)$ is bounded above by the number of prime divisors of n (counted with multiplicity).

(b) If N is a normal subgroup of G, then $l(G) = l(N) + l(G/N)$. (To get an inequality one way round, we take a subgroup chain passing through N. The other way, note that if $H, K \leq G$ with $H < K$, then either $H \cap N < K \cap N$ or $HN/N < KN/N$; so every step in a longest chain for G involves a move in either a chain for N or a chain for G/N.

From the second point, we see that $l(G)$ is the sum of the lengths of the composition factors of G; so it suffices to compute $l(G)$ for all simple groups G. Sometimes it is more convenient to go the other way, e.g. calculate $l(S_n)$ and subtract one to get $l(A_n)$.

In the early 1980s, a remarkable formula for the length of the symmetric group S_n was found. This was published in the paper [14].

Theorem 5.1 (uses CFSG) *The length of the symmetric group S_n is*

$$l(S_n) = \left\lfloor \frac{3n}{2} \right\rfloor - b(n) - 1,$$

where $b(n)$ is the number of 1*s in the base* 2 *representation of n.*

Proof I outline the proof. The first task is to find a chain of length equal to the right-hand side of the displayed equation. This can be done using two kinds of steps $S_{k_1+k_2} > S_{k_1} \times S_{k_2}$, and $S_{2k} > S_k \wr S_2 > S_k \times S_k$. The strategy is as follows. First, write n in base 2, as a sum of distinct powers of 2:

$$n = 2^{a_1} + 2^{a_2} + \cdots + 2_{a_r}.$$

Then $r-1$ steps of the first type descend to $S_{2^{a_1}} \times \cdots \times S_{2^{a_r}}$. Then we apply the second step to each factor, descending from S_{2^a} to $S_{2^{a-1}} \times S_{2^{a-1}}$ in two steps if $a > 1$, and repeating until we reach the identity. (Note that we get from S_2 to the identity in one step.) Careful bookkeeping now shows that the claimed length is achieved.

For the converse, we have to show that no longer chain is possible. We use induction on n in the course of the proof. Suppose that the first step in a chain is $S_n > H$. Then H is a maximal subgroup of S_n. We check the possibilities.

- If H is intransitive, then $H = S_k \times S_{n-k}$ for some k, and we can bound the lengths of S_k and S_{n-k} by induction.
- If H is imprimitive, then $H = S_k \wr S_l$ for some k,l with $kl = n$; again we can use induction.
- Now we can assume that H is primitive, and apply the O'Nan–Scott Theorem. If H is non-basic, then $H = S_k \wr S_l$ for some k,l with $k^l = n$; again induction applies.
- If H is affine or diagonal, or an almost simple group other than S_m on k-sets or A_n, then known bounds on the order show that the chain cannot be too long.
- If $H = S_m$ on k-sets, with $n = \binom{m}{k}$, use induction.
- Finally, if $H = A_n$, we let the next step in the chain be $A_n > K$, and apply the same analysis to K (except that the last case no longer applies).

□

The CFSG is probably not necessary in this proof. Elementary bounds not depending on CFSG by Babai and Pyber [9, 27] are enough to give a bound on n, but this bound is a little too large for analysis of all n up to the bound to be practicable.

Another consequence of CFSG is the determination of all groups G for which $l(G)$ is equal to the number of prime divisors of G counted with multiplicity. As noted earlier, it suffices to find all the simple groups with this property. If G is such a simple group, then the first step in a maximal chain in G is of the form $G > H$, where H is a maximal subgroup of G and has prime index in G. So G is isomorphic to a permutation group of prime degree. A theorem of Burnside, mentioned earlier, shows that G is either cyclic of prime order or 2-transitive. From CFSG we can read off a list of 2-transitive simple groups. We further filter this list since H must have the properties that its composition factors are also simple groups of prime degree. The final list of composition factors is

- C_p, for p prime;
- $\mathrm{PSL}(2,2^a)$ where 2^a+1 is a Fermat prime;
- $\mathrm{PSL}(2,7)$, $\mathrm{PSL}(2,11)$, $\mathrm{PSL}(3,3)$ and $\mathrm{PSL}(3,5)$.

It was surprisingly long before attempts were made to extend these results to semigroups. In particular, we have a simple formula for the length of S_n; are there analogous formulae for the length of the full transformation semigroup T_n and the symmetric inverse semigroup I_n? These questions, among others, were tackled in [13], from which the following discussion is taken. While we clearly have $l(G) \leq \log_2 |G|$ for a group G, this can fail for semigroups; the zero semigroup has length one less than its order.

Theorem 7.2 of that paper gives a formula for the length of any inverse semigroup in terms of the lengths of various groups involved in it. In particular,

$$l(I_n) = -1 + \sum_{i=1}^{n+1} \left[\binom{n}{i-1} (l(S_{i-1}) + 2) + \binom{n}{i-1} \left(\binom{n}{i-1} - 1 \right) \frac{(i-1)!}{2} - 1 \right].$$

From this it follows that

$$\lim_{n\to\infty} \frac{l(I_n)}{|I_n|} = \frac{1}{2}.$$

The proofs of these results use some detailed semigroup theory. By contrast, there is no known formula for $l(T_n)$, and the estimates obtained so far are purely combinatorial. In fact, it is shown that $l(T_n)/|T_n|$ is asymptotically bounded below by a non-zero constant; the analysis gives the constant e^{-2}, but this is probably not best possible.

The strategy is to find a chain which passes through the subsemigroups $T_{n,k}$ consisting of all maps of rank at most k. Now $T_{n,k}$ is an ideal in T_n, and we can identify the quotient $T_{n,k}/T_{n,k-1}$ with the semigroup $T^*_{n,k}$ defined as follows: the elements are all the maps of rank k, together with an additional element 0; the product of two maps of rank k is equal to their product in T_n if it has rank k, and is 0 otherwise.

Let f_1 and f_2 be two maps of rank k, with images A_1 and A_2 and kernels P_1 and P_2. As we have seen, $f_1 f_2$ has rank k if and only if A_1 is a transversal for P_2. So, if we can find sets $\mathscr{A}$ and $\mathscr{P}$ of k-sets and k-partitions with the property that no element of $\mathscr{A}$ is a section for any element of $\mathscr{P}$, then the maps with images in $\mathscr{A}$ and kernels in $\mathscr{P}$ will form a zero semigroup in $T^*_{n,k}$, and will have a chain of subsemigroups of length one less than its order.

Define a *league* to be a pair $(\mathscr{A},\mathscr{P})$, where $\mathscr{A}$ and $\mathscr{P}$ are sets of k-sets and k-partitions such that no member of $\mathscr{A}$ is a section for any member of $\mathscr{P}$. We measure the "size" of a league by the product of the cardinalities of $\mathscr{A}$ and $\mathscr{P}$, which is called the *content* of the league. (The number of elements in our zero semigroup is the content of the league times $k!$.)

Problem What is the maximum content of a league (in terms of n and k)?

The league used to obtain the lower bound for $l(T_n)$ cited above is defined as follows: $\mathscr{P}$ is the set of all k-partitions having n as a singleton part; $\mathscr{A}$ is the set of all k-sets not containing n. This has cardinality $\binom{n-1}{k}S(n-1,k-1)$, where S is the Stirling number of the second kind. The paper also includes some discussion of the combinatorial problem. For small k, this league has smaller content than the league defined as follows: $\mathscr{A}$ is the set of k-subsets containing 1 and 2, and $\mathscr{P}$ is the set of all k-partitions not separating 1 and 2. This league has content $\binom{n-2}{k-2}S(n-1,k)$.

5.2 Further topics

5.2.1 Between primitive and 2-homogeneous

We saw in Chapter 3 two classes of permutation groups lying strictly between primitive and 2-homogeneous: synchronizing groups, and separating groups. These classes are not the same, but every separating group is synchronizing, and we know only finitely many examples of synchronizing groups which are not separating.

Some further classes are introduced in [8], including *partition-separating* and *spreading*. They are also related to some classes defined elsewhere, such as $\frac{3}{2}$-*transitive* and $\mathbb{Q}I$. The groups in these two classes have recently been determined.

The one remaining inclusion which has not been shown to be proper is between the classes of spreading and $\mathbb{Q}I$ groups. I refer to the paper for definitions.

The definition of $\mathbb{Q}I$ involves representation theory over $\mathbb{Q}$, and is the equivalent of 2-homogeneous and 2-transitive for representations over $\mathbb{R}$ and $\mathbb{C}$. There are a number of open problems on these representation-theoretic concepts.

A different class of groups between primitive and 2-homogeneous arose in an investigation of association schemes [1, 12], and were named *AS-free*. These are groups which preserve no non-trivial association scheme on their domain. It is not known what is their relationship, if any, to synchronizing groups and their friends.

The paper [8] contains a long list of problems about these groups.

5.2.2 Going down

It is trivial that a k-transitive group is $(k-1)$-transitive for $k \leq n$. We outlined in Chapter 4 the lovely and elementary proof that a k-homogeneous group is $(k-1)$-homogeneous for $k \leq n/2$.

We also saw in that chapter the k-universal transversal property of a permutation group, the fact that the k-ut implies the $(k-1)$-ut with a very few exceptions (though this is much more difficult to prove), and the importance of this implication for semigroup theory. We also touched on the property of $(k-1,k)$-homogeneity, and the fact that this implies $(k-2,k-1)$-homogeneity with a few exceptions. Finally, we met the k-existential transversal property, where it is not known whether it implies the $(k-1)$-et property (although a complicated argument using CFSG implies that groups with the k-et must be symmetric or alternating for $8 \leq k \leq n/2$).

So a few questions naturally occur:

- Find elementary proofs (not using CFSG) that k-ut implies $(k-1)$-ut, and that $(k-1,k)$-homogeneous implies $(k-2,k-1)$-homogeneous.
- Prove that k-et implies $(k-1)$-et (preferably without CFSG).
- Are there other similar properties where such results might hold?

5.3 Open problems

5.3.1 Synchronization

Apart from the ultimate problem of proving the Černý conjecture, here are some (possibly more approachable) problems on Chapter 3.

- Is it the case that a primitive permutation group of degree n synchronizes any map of rank greater than $n/2$? (The best we know in this direction is

the result that a primitive group synchronizes maps of rank at least $n-4$. Note that a map of rank greater than $n/2$ is necessarily non-uniform.)

- Are there infinitely many primitive groups which synchronize non-uniform maps of rank 5? (Here 5 is the smallest such rank possible.)
- Classify the primitive groups which fail to synchronize a map of rank 3 (this is the smallest possible such rank).
- We say that a number k is a *non-synchronizing rank* for the transitive group G if there is a map of rank k not synchronized by G. Let $\mathrm{NS}(G)$ be the set of all non-synchronizing ranks for G. It is known that, if G is imprimitive, then $|\mathrm{NS}(G)| \geq (\frac{3}{4} - o(1))n$. It is conjectured that, for primitive groups G, $|NS(G)| = o(n)$. Examples in [4] have about $\sqrt{n}$ non-synchronizing ranks. These groups are non-basic, and it is conjectured that, for basic primitive groups, the number of non-synchronizing ranks might be as small as $O(\log n)$.
- Prove the Černý conjecture for automata whose transitions are generators of a primitive permutation group together with a single non-permutation.

5.3.2 Regularity and idempotent generation

The ultimate question in this line of activity is the following (the five parts are all distinct): Classify all pairs (G, f) for which

(a) $\langle G, f\rangle \setminus G$ is regular;

(b) $\langle G, f\rangle \setminus G$ is idempotent-generated;

(c) $\langle g^{-1}fg : g \in G\rangle$ is regular;

(d) $\langle g^{-1}fg : g \in G\rangle$ is idempotent-generated;

(e) $\langle G, f\rangle \setminus G = \langle g^{-1}fg : g \in G\rangle$.

Failing a complete solution, we can ask for the appropriate condition to hold for all maps with a given image, or a given kernel, or of a given rank. There are plenty of problems here to engage with! As we noted, a weaker condition than asking for the semigroup to be regular is asking for f to be a regular element of the semigroup; as we saw, it is quite difficult to pass from "f regular in S" to "S regular".

5.3.3 Other topics

- Prove the conjecture that, if S is a transformation semigroup whose group of units is a primitive permutation group, then all automorphisms of S are induced by elements of its normaliser in the symmetric group.

- Improve the lower bound for the length of a chain of semigroups in the full transformation semigroup T_n. In particular, show that $l(T_n)/|T_n|$ tends to a limit as $n \to \infty$, and find this limit.

5.4 Books

These books cover the background material for the notes, and have been referred to at relevant points throughout the notes. Papers are listed in the following Bibliography.

(A) R. A. Bailey, *Association Schemes: Designed Experiments, Algebra and Combinatorics*, Studies in Advanced Mathematics **84**, Cambridge University Press, 2004.

(B) P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts **45**, Cambridge University Press, 1999.

(C) J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer, 1996.

(D) P. Hell and J. Nešetřil, *Graphs and Homomorphisms*, Oxford University Press, 2004.

(E) J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, 2nd edition, Springer, 2016.

(F) J. M. Howie, *Fundamentals of Semigroup Theory*, LMS Monographs **12**, Oxford University Press, 1995.

(G) D. E. Taylor, *The Geometry of the Classical Groups*, Helderman, Berlin, 1992.

(H) R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics **251**, Springer, 2009.

Bibliography

[1] P. P. Alejandro, R. A. Bailey and P. J. Cameron, Association schemes and permutation groups, *Discrete Math.* **266** (2003), 47–67.

[2] J. André, J. Araújo and P. J. Cameron, The classification of partition homogeneous groups with applications to semigroup theory, *J. Algebra* **452** (2016), 288–310.

[3] J. Araújo, W. Bentz and P. J. Cameron, Orbits of primitive k-homogenous groups on $(n-k)$-partitions with applications to semigroups, `https://arxiv.org/abs/1512.05608`

[4] J. Araújo, W. Bentz, P. J. Cameron, G. F. Royle and A. Schaefer, Primitive groups, graph endomorphisms and synchronization, *Proc. London Math. Soc.* **113** (2016), 829–867.

[5] J. Araújo and P. J. Cameron, Two generalizations of homogeneity in groups with applications to regular semigroups, *Trans. Amer. Math. Soc.* **368** (2016), 1159–1188.

[6] J. Araújo and P. J. Cameron, Primitive groups, road closures and idempotent generation, `https://arxiv.org/abs/1611.08233`

[7] J. Araújo, P. J. Cameron, M. Neunhöffer and J. D. Mitchell, The classification of normalizing groups, *J. Algebra* **373** (2013), 481–490.

[8] J. Araújo, P. J. Cameron and B. Steinberg, Between primitive and 2-transitive: Synchronization and its friends, `https://arxiv.org/abs/1511.03184`

[9] L. Babai, On the order of uniprimitive permutation groups, *Ann. Math.* (2) **113** (1981), 553–568.

[10] K. D. Blaha, Minimal bases for permutation groups: the greedy approximation, *J. Algorithms* **13** (1992), 297–306.

[11] T.C. Burness, M.W. Liebeck and A. Shalev, Base sizes for simple groups and a conjecture of Cameron, *Proc. London Math. Soc.* **97** (2009), 116–162.

[12] P. J. Cameron, Coherent configurations, association schemes and permutation groups, pp. 55–71 in Groups, Combinatorics and Geometry (ed. A. A. Ivanov, M. W. Liebeck and J. Saxl), World Scientific, Singapore, 2003.

[13] P. J. Cameron, M. Gadouleau, J. D. Mitchell, and J. Peresse, Chains of subsemigroups, *Israel J. Math.*, in press.

[14] P. J. Cameron, R. Solomon and A. Turull, Chains of subgroups in symmetric groups, *J. Algebra* **127** (1989), 340–352.

[15] J. Černý, Poznámka k homogénnym eksperimentom s konecnými automatami [A remark on homogeneous experiments with finite automata], *Mat.-Fyz. Časopis Slovensk. Akad. Vied.* **14** (1964), 208–216.

[16] E. Dobson and A. Malnič, Groups that are transitive on all partitions of a given shape, *J. Algebraic Combinatorics* **42** (2015), 605–617.

[17] Christoph Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geometriae Dedicata* **2** (1974), 425–460.

[18] W. M. Kantor, 4-homogeneous groups, *Math. Z.* **103** (1968), 67–68.

[19] W. M. Kantor, *k*-homogeneous groups, *Math. Z.* **124** (1972), 261–265.

[20] W. M. Kantor and R. A. Liebler, The rank 3 permutation representations of the finite classical groups, *Trans. Amer. Math. Soc.* **271** (1982), 1–71.

[21] A. Laradji and A. Umar, Combinatorial results for the symmetric inverse semigroup, *Semigroup Forum* **75** (2007), 221–236.

[22] Martin W. Liebeck, The affine permutation groups of rank three, *Proc. London Math. Soc.* (3) **54** (1987), 477–516.

[23] Martin W. Liebeck and Jan Saxl, The finite primitive permutation groups of rank 3, *Bull. London Math. Soc.* **18** (1986), 165–172.

[24] D. Livingstone and A. Wagner, Transitivity of finite permutation groups on unordered sets, *Math. Z.* **90** (1965), 393–403.

[25] A. Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.

[26] W. J. Martin and B. E. Sagan, A new notion of transitivity for groups and sets of permutations, *J. London Math. Soc.* **73** (2006), 1–13.

[27] L. Pyber, The orders of doubly transitive permutation groups: elementary estimates, *J. Combinatorial Theory* (A) **62** (1993), 361–366.

[28] I. K. Rystsov, Quasioptimal bound for the length of reset words for regular automata, *Acta Cybernet.* **12** (1995), 145–152.

[29] R. P. Sullivan, Automorphisms of transformation semigroups. *J. Australian Math. Soc.* **20** (1975), 77–84.

[30] M. V. Volkov, Synchronizing automata and the Černý conjecture, LATA 2008, LNCS 5196 (2008), 11–27.

Index