Chains of subsemigroups

Peter J. Cameron, St Andrews
in collaboration with Maximilien Gadouleau, Durham
James Mitchell, St Andrews
Yann Peresse, Hertfordshire

Aberdeen Algebra Seminar, 26 February 2015

A surprising formula

Theorem

The length of the longest chain of subgroups in the symmetric group S_n is

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

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

I proved this in the early 1980s; Ron Solomon and Alex Turull proved it independently; we joined forces to write it up.

The $b(n)$ suggests how to find a longest chain:

- If $n = 2^{a_1} + \cdots + 2^{a_r}$, where the a_i are distinct (and $r = b(n)$), then descend to $S_{2^{a_1}} \times \cdots \times S_{2^{a_r}}$ in $r - 1$ steps.
- $S_{2^a} > S_{2^{a-1}} \wr S_2 > S_{2^{a-1}} \times S_{2^{a-1}}$ for $a > 1$.
- Then do the bookkeeping.

The Classification of Finite Simple Groups is needed to show that there is no longer chain; its use could probably be avoided.

For some n (for example 7 and 15) there are other chains of the same length.

Subgroup length

Define $l(G)$ to be the length of the longest chain of subgroups in G.
Another interpretation: $l(G)$ is the maximum, over all permutation actions of G, of the size of a largest irredundant base (a sequence of points whose pointwise stabiliser is the identity, with no point fixed by the stabiliser of its predecessors).
A trivial observation: by Lagrange's Theorem, $l(G)$ does not exceed the number of prime divisors of $|G|$ (counted with multiplicity).
The question of finding $l(S_n)$ was first raised by László Babai in the context of computational group theory.

It is easy to see that, if $N \trianglelefteq G$, then $l(G) = l(N) + l(G/N)$. (It is trivial that $l(G) \geq l(N) + l(G/N)$, by taking a chain passing through N. For the reverse inequality, observe that any step $H < K$ entails either $H \cap N < K \cap N$ or $HN/N < KN/N$, and so requires a step in either N or G/N.) Hence we can find $l(G)$ if we know the lengths of composition factors of G.

Solomon and Turull, with various co-authors, have worked out exact values or good bounds for all the finite simple groups.

So, in what follows, we shall typically regard the length of a group as "known".

Semigroups

The length of a group G is at most the logarithm of $|G|$, by Lagrange's Theorem. No such bound holds for semigroups. The extreme case is the zero semigroup Z, containing an element 0 and having the property that any product is equal to 0. Then every subset containing 0 is a subsemigroup, and the length of the longest chain of non-empty semigroups is $|S| - 1$. Can we calculate the maximum length of a chain in such naturally-occurring semigroups as, for example,

- T_n, the full transformation semigroup on n points, consisting of all maps from the domain $\{1, \ldots, n\}$ to itself (with order $|T_n| = n^n$), or
- I_n, the symmetric inverse semigroup on n points, consisting of all bijections between pairs of subsets of the domain $\{1, \ldots, n\}$ of the same cardinality (with order $|I_n| = \sum_{i=0}^{n} \binom{n}{i}^2 i!$)?

It turns out that for both T_n and I_n, the length is a constant multiple of the order. (The proof techniques are quite different. For I_n we have an exact formula for the length, in terms of $l(S_k)$ for $k \leq n$, and the result is asymptotically $\frac{1}{2}|I_n|$. For T_n we only have the weaker result that $l(T_n) \geq c|T_n|$ for an explicit $c > 0$, and cannot prove yet that $l(T_n)/|T_n|$ tends to a limit.)

First, a point of terminology. Unlike for groups, the empty set is a subsemigroup of any semigroup. For convenience, we redefine length so that $l(S)$ is the largest number of non-empty semigroups in a chain minus 1. This definition does what you expect for groups and monoids, and makes some formulae simpler to state and use.

A general result . . .

It is clear that, if T is a subsemigroup of S, then $l(T) \leq l(S)$. Quotients are more difficult. The "kernel" of a group homomorphism is a special kind of subgroup, but the kernel of a semigroup homomorphism is a congruence (a partition of S). It is true that, if ρ is a congruence on S, then $l(S/\rho) \leq l(S)$. The best analogue of the result $l(G) = l(N) + l(G/N)$ that we have for semigroups is the following. An ideal of a semigroup S is a subset I closed under left and right multiplication by elements of S. It is a subsemigroup. There is also a *Rees quotient* S/I, defined as follows: the elements are those of $S \setminus I$ together with a new element 0; the product xy is equal to its value in S unless this lies in I, in which case the product in S/I is zero.

Theorem

If I is an ideal of a semigroup S, then $l(S) = l(I) + l(S/I)$.

. . . and a corollary

A semigroup S is regular if for every $x \in S$ there exists $y \in S$ such that $xyx = x$.
We also need Green's relations. If S is a semigroup, let S^1 be the monoid obtained by adjoining an identity if there is not one already. Then two elements x and y are $\mathcal{L}$-equivalent (resp. $\mathcal{R}$-equivalent, $\mathcal{J}$-equivalent) if $S^1x = S^1y$ (resp., $xS^1 = yS^1$, $S^1xS^1 = S^1yS^1$). The $\mathcal{L}$-, $\mathcal{R}$- and $\mathcal{J}$-classes are the equivalence classes of these relations.
The principal factor of a $\mathcal{J}$-class J has elements $J \cup \{0\}$, with xy equal to its value in S if this lies in J, 0 otherwise.

Theorem

Let S be a finite regular semigroup with $\mathcal{J}$-classes $J_1, \ldots J_m$. Then

$$l(S) = l(J_1^*) + \cdots + l(J_m^*) - 1.$$

Inverse semigroups

An inverse semigroup is a semigroup S such that, for any $x \in S$, there exists a (unique) $y \in S$ such that $xyx = x$ and $yxy = y$. Inverse semigroups are regular, so the preceding result applies:

Theorem

Let S be an inverse semigroup with $\mathcal{J}$-classes $J_1, \ldots, J_m$. If n_i denotes the numebr of $\mathcal{L}$- and $\mathcal{R}$-classes contained in J_i, and G_i is any maximal subgroup of S contained in J_i, then

$$l(S) = -1 + \sum_{i=1}^{m} \left(n_i(l(G_i) + 2) + \binom{n_i}{2} |G_i| - 1 \right).$$

The symmetric inverse semigroup

For the semigroup I_n of partial bijections between subsets of $\{1,\ldots,n\}$, we define the rank of an element to be the cardinality of the subsets between which it maps.
Two elements are $\mathcal{J}$-equivalent if and only if they have the same rank. So if J_i is the class of maps of rank i, then $\mathcal{L}$ and $\mathcal{R}$ are determined by the domain and range of the maps in J_i, so $n_i = \binom{n}{i}$, and $G_i = S_i$.
Thus

$$l(I_n) = -1 + \sum_{i=0}^{n} \left(\binom{n}{i} (l(S_i)+2) + \binom{n}{i} \left(\binom{n}{i} - 1 \right) \frac{i!}{2} - 1 \right).$$

This formula is due to Ganyushkin and Mazorchuk by a different argument. Note that $l(S_i)$ is given by the formula of Cameron, Solomon and Turull.

Some values

n	1	2	3	4	5	6	7	8
$\|I_n\|$	2	7	34	209	1546	13327	130922	1441729
$l(I_n)$	1	6	25	116	722	5956	59243	667500

We used the formula to show that

Theorem

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

The same limit holds for various other interesting semigroups: the dual inverse symmetric semigroup, the semigroup of partial order-preserving injective mappings, and the semigroup of partial orientation-preserving injective mappings.

The full transformation monoid

For T_n, our results are much less precise. Recall that $|T_n| = n^n$.

Theorem

$l(T_n)/|T_n| \geq \mathrm{e}^{-2} - n^{-1/3}(2\mathrm{e}^{-2}(1-\mathrm{e}^{-1}) + o(1))$.

Again it is true that T_n is regular, so $l(T_n)$ is the sum of the lengths of the principal factors of its $\mathcal{J}$-classes, minus 1. Again it is true that the elements of given rank k form a $\mathcal{J}$-class, which we denote by J_k.

An element $f \in T_n$ with rank k has a kernel, a k-partition of $\{1, \ldots, n\}$, and an image, a k-subset of $\{1, \ldots, n\}$. Now the product $f_1 f_2$ has rank k if and only if the image of f_1 is a transversal for the kernel of f_2, and has smaller rank (and so is 0 in the principal factor) otherwise.

Leagues

A league of rank k on $\{1, \ldots, n\}$ is a pair (P, S), where P is a set of k-partitions of the domain and S a set of k-subsets, with the property

no member of S is a transversal for any member of P.

The content of a league (P, S) is $|P| \cdot |S|$.
Given a league (P, S) with content c, we have a zero semigroup of order $ck!$ in J_k^*. Hence

Proposition

Let $F(n, k)$ be the largest league of rank k on $\{1, \ldots, n\}$. Then

$$l(T_n) \geq \sum_{k=1}^{n} F(n, k)k! - 1.$$

Leagues with large content

There are several constructions for leagues with large content; which is best depends on the relative sizes of n and k.

- Choose one element of $\{1, \ldots, n\}$, say 1. Let P be the set of all k-partitions having 1 as a singleton part, and S the set of all k-subsets not containing 1. Then (P, S) is a league, with content $\binom{n-1}{k} S(n-1, k-1)$, where S denotes Stirling numbers of the second kind ($S(n, k)$ is the number of k-partitions of $\{1, \ldots, n\}$).
- Choose two elements of $\{1, \ldots, n\}$, say 1 and 2. Let S consist of all k-sets containing 1 and 2, and P the k-partitions which don't separate these two points. Then (S, P) is a league, with content $\binom{n-2}{k-2} S(n-1, k)$.

The first strategy is better for large k, the second for small k.

Open problems

Problem

Calculate $F(n,k)$, the largest content of a league of rank k on n points.

We have exact results for $k \leq 2$ and $k \geq n-1$, and the following:

n	$k=2$	3	4	5	6
3	1				
4	3	3			
5	9	28	6		
6	21	150	125	12	
7	45	760	1350	390	20

Problem

Does $l(T_n)/|T_n|$ tend to a limit as $n \to \infty$? Is the limit e^{-2}?

Clearly our bounds could be tightened a little.

Other semigroups

Similar techniques apply to the semigroup O_n of order-preserving transformations of $\{1, \ldots, n\}$, where we have a lower bound which is asymptotically $|O_n|/4$. (Note that $|O_n| = \binom{2n-1}{n}$.)

We also have results for the general linear semigroup (all linear maps on $\mathrm{GF}(q)^n$), Brandt semigroups, Rees matrix semigroups, free bands …

Numbers of subsemigroups

The number of subgroups of the symmetric group S_n is at least roughly $2^{n^2/16}$.
A remarkable result of Pyber found an upper bound also of the form 2^{cn^2} for the number of subgroups.
For a semigroup S, as we have seen, the number can be within a constant factor of $2^{|S|}$. How many subsemigroups does, for example, T_n have?

Theorem

For an explicit constant c, the number of subsemigroups of T_n is at least $2^{(c-o(1))n^{n-1/2}}$, where

$$c = \frac{\mathrm{e}^{-2}}{3\sqrt{3(\mathrm{e}^{-1} - 2\mathrm{e}^{-2})}}.$$

Note that this is a bit smaller than $2^{c|T_n|}$ (because of the $-1/2$ in the exponent).

Generators

Theorem

The smallest number $d(n)$ such that any subsemigroup of T_n can be generated by $d(n)$ elements is at least $(c - o(1))n^{n-1/2}$, where c is as in the preceding theorem.

The corresponding parameter for S_n is much smaller. Annabel McIver and Peter Neumann showed:

Theorem

For $n \geq 4$, any subgroup of S_n can be generated by at most $\lfloor n/2 \rfloor$ elements.

Mark Jerrum gave the weaker bound $n - 1$, but with an algorithmic proof. Given a sequence of elements of S_n, we can read each element and do a polynomial-time computation producing at most $n - 1$ elements generating the same group.

Whiston's theorem

A similar-looking theorem was proved by Julius Whiston. A set of elements of a group is independent if no element lies in the subgroup generated by the others.

Theorem

An independent set in S_n has size at most $n-1$, with equality if and only if it generates the group.

This group parameter arose in the analysis of the product replacement algorithm by Diaconis and Saloff-Coste. Philippe Cara and I found all independent sets meeting Whiston's bound.

Other group parameters

We saw much earlier that the length of a group G is the maximum of the size of a largest irredundant base, over all permutation actions of G. This suggests two related parameters:

- the maximum, over all actions, of the maximum size of a minimal base;
- the maximum, over all actions, of the minimum base size.

Little is known about the second parameter, but the first has another interpretation …

Boolean sublattices

Theorem

Let G be a finite group.

- *The largest size of an independent subset of G is equal to the maximum m for which the Boolean lattice $B(m)$ is embeddable as a join-semilattice of the subgroup lattice of G.*
- *This is equal to the maximum m for which the Boolean lattice $B(m)$ is embeddable as a meet-semilattice of the subgroup lattice of G.*
- *The maximum, over all actions of G, of the maximum size of a minimal base, is equal to the maximum m for which the Boolean lattice $B(m)$ is embeddable as a meet-semilattice of the subgroup lattice of G in such a way that the bottom element is a normal subgroup.*

Two problems

Problem
Are the two parameters in the above theorem equal for any group G?

Problem
Is there an analogue for transformation semigroups?