Combinatorics of inverse semigroups

This is an exposition of some results explained to me by Abdullahi Umar, together with some further speculations of my own and some with Nik Ruskuc.

1 Inverse semigroups and orders

For the first part, I take a nineteenth-century view of algebra: a group will be a permutation group, for example.

- A *permutation group* on X is a non-empty set of permutations of X closed under composition and inversion. The set of all permutations is a group, the *symmetric group* $S(X)$.
- A *transformation semigroup* on X is a non-empty set of transformations of X (maps from X to X), closed under composition. The set of all transformations is a semigroup, the *transformation semigroup* $T(X)$.
- An *inverse semigroup of partial permutations* on X is a non-empty set of partial permutations (bijections between subsets) of X, closed under composition and inversion. (Composition is defined wherever possible: x^{fg} is defined if $x^f = y$ is defined and is in the domain of g; then $x^{fg} = y^g$.) The set of all partial permutations is an inverse semigroup, the *symmetric inverse semigroup* $P(X)$.

It is a truism that groups measure symmetry. But the word "symmetry" has a local as well as a global meaning (i.e. "correspondence of parts"), and with this meaning, inverse semigroups are more appropriate.

The first theorem gives the orders of our basic structures.

Theorem 1 *Let $|X| = n$. Then*

(a) $|S(X)| = n!$;

(b) $|T(X)| = n^n$;

(c) $|P(X)| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$.

Proof All straightforward except possibly (c): once the domain and range are chosen there are $k!$ bijections between them.

The expression for $|P(X)|$ does not have a simple closed form, and in particular is not equal to $|T(X)|$. For $n = 2$, $|T(X)| = 4$ while $|P(X)| = 7$.

We can define some interesting sub-semigroups of $P(X)$ by means of a total order on X. A partial permutation f is *monotone* if $x < y$ implies $x^f < y^f$ if both are defined; it is *decreasing* if $x^f \leq x$ for all x in the domain of f, and *strictly decreasing* if $x^f < x$ for all such x. We let $P_m(X)$, $P_d(X)$ and $P_s(X)$ denote the semigroups of monotone, decreasing, and strictly decreasing elements respectively; and $P_{md}(X) = P_m(X) \cap P_d(X)$, $P_{ms}(X) = P_m(X) \cap P_s(X)$. Now we have:

Theorem 2 *Let $|X| = n$. Then*

- $|P_m(X)| = \binom{2n}{n}$;
- $|P_d(X)| = B_{n+1}$ *and* $|P_s(X)| = B_n$, *where B_n is the nth Bell number (the number of partitions of an n-set);*
- $|P_{md}(X)| = C_{n+1}$ *and* $|P_{ms}(X)| = C_n$, *where C_n is the nth Catalan number.*

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 familiar binomial 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 Catalan object. The Catalan numbers, given by the formula $C_n = \frac{1}{n+1}\binom{2n}{n}$, count many different things. I will use the interpretation as *ballot numbers*: C_n is the number of ways that the votes in an election where two candidates A and B each obtain n votes, if A is never behind B at any point during the count. For example, $C_2 = 2$, since the count may be ABAB or AABB.

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 $i \notin \mathrm{Ran}(f)$,

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

BB, 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 solutions to the ballot problem. (It is necessary to show that the resulting string has equally many As and Bs, but 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 (c), also $P_{md}(n) = C_{n+1}$.

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

2 A linear analogue

Let q be a prime power, and let V be an n-dimensional vector space over the Galois field $\mathrm{GF}(q)$ of order q. The number of k-dimensional subspaces of V is the *Gaussian coefficient*

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

We have linear analogues of the previous objects. Corresponding to the symmetric group is the *general linear group* $\mathrm{GL}(n,q)$ of invertible linear maps on V; its order is

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

For temporary convenience, we let $T(n,q)$ denote the semigroup of all linear maps on V, and $P(n,q)$ the inverse semigroup of linear bijections between subspaces of V. Now something rather different happens:

Theorem 3 $|S(n,q)| = |P(n,q)|$.

Proof We specify an element of $P(n,q)$ by choosing two k-dimensional subspaces of V and an isomorphism between them; so

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

the q-analogue of the formula for $|P(n)|$ given earlier.

We specify an element of $S(n,q)$ by giving its image, a k-dimensional subspace W of $V = V(n,q)$, and its kernel, a $(n-k)$-dimensional subspace U of V, and an isomorphism from V/U to W. So

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

But $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$ by duality, so these two expressions are equal.

We deduce the following identity:

Corollary 4

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

We obtain further semigroups by following the procedure of Laradji and Umar. Here are some initial thoughts on this.

Let $V = V(n,q)$, and suppose that a total order of V is given. Let $P_m(V)$ denote the set of monotonic isomorphisms between subspaces of V.

Theorem 5 *For any ordering of V, we have*

$$|P_m(V)| \leq \sum_{k=0}^{n} \begin{bmatrix} n \\ mk \end{bmatrix}_q^2,$$

with equality if and only if the unique order-preserving bijection between any two subspaces of the same dimension is linear.

The proof is obvious, so we are led to ask:

Problem Given the vector space $V = V(n,q)$, how many orderings of V have the property that the unique order-preserving bijection between any two subspaces of the same dimension is linear, and how many inequivalent inverse semigroups $P_m(V)$ do they define? Call such an ordering of V *compatible*.

Here are a couple of observations.

Theorem 6 *(a) Compatible orderings always exist. Indeed, take any ordering of the field $\mathrm{GF}(q)$; then the lexicographic order of $\mathrm{GF}(q)^n$ is compatible.*

(b) In any compatible ordering, there is an integer k with $0 \leq k \leq q-1$, the zero vector is in position $1 + k(q^n - 1)/(q-1)$.

(c) Any ordering of $V(1,q)$ are compatible.

(d) All compatible orderings of $V = V(2,q)$ are found by the following procedure: Take any ordering of $\mathrm{GF}(q)$; translate this to all the 1-dimensional subspaces of V; then extend the resulting partial order to a total order of V in any manner (it is possible to count the number of such orderings).

Proof (a) We use the fact that every subspace of $\mathrm{GF}(q)^n$ has a unique basis in reduced echelon form. Let W be a k-dimensional subspace, and suppose that the leading ones in the reduced echelon basis occur in positions $m_1, m_2, \ldots, m_k$. Then projection of W onto these coordinates is a vector space isomorphism to $\mathrm{GF}(q)^k$. I will show that it is also an order-isomorphism from the induced ordering on W to the lexicographic ordering on $\mathrm{GF}(q)^k$.

Take two vectors of W. Since their difference is in W, its first non-zero entry is in position m_i for some i; in other words, the two vectors differ first in position m_i, so to decide their order we simply need to compare the order of their m_i coordinates in the field. This is precisely the lexicographic order on the projection onto these coordinates.

This already gives us a range of orders, since the field has $q!$ orderings. However, all these orderings define the same inverse semigroup: if two subspaces W_1 and W_2 have the same dimension, then the unique order-preserving map between them maps the reduced echelon basis of W_1 to that of W_2.

(b) Since all 1-dimensional subspaces are isomorphic, there is an integer k with $0 \le k \le q-1$ such that 0 is the $(k+1)$-st element of each 1-dimensional subspace.

Thus, in the ordering of V, each of the $(q^n-1)/(q-1)$ 1-dimensional subspaces contains exactly k elements before 0 and $q-k-1$ after it. So V contains $k(q^n-1)/(q-1)$ elements before 0 and $(q-k-1)(q^n-1)/(q-1)$ elements after it.

Every value of k can occur here: simply take the construction in (a), where 0 is the $(k+1)$-st element of the field.

(c) The identity map is always linear.

(d) It is clear that the ordering of elements in the same 1-dimensional subspace must be as specified; and by the argument in (c), the ordering of elements is entirely unrestricted.

To count these orderings, proceed as follows. First we order the field so that 0 is in position $k+1$; without loss we may assume that 1 is in the first available position. There are $(q-2)!$ such orderings.

Now choose a distinguished element in each 1-dimensional subspace (in $(q-1)^{q+1}$ ways), and transfer the ordering of the field to this subspace so that the chosen element corresponds to 1.

Now there are $(q+1)k$ elements less than 0, and $(q+1)(q-k-1)$ elements greater than 0. Order these sets respecting the orders on the 1-dimensional subspaces. The numbers of ways are multinomial coefficients, for example,

$\binom{(q+1)k}{k,k,\ldots,k}$ for the elements less than 0.

We conclude that the number of compatible orderings of $V(2,q)$ is

$$(q-2)!\,(q-1)^{q+1}\sum_{k=0}^{q-1}\binom{(q+1)k}{k,k,\ldots,k}\binom{(q+1)(q-k-1)}{q-k-1,\ldots,q-k-1}.$$

For $q=2$, we see that the zero element must be first or last, and part (c) shows that any ordering of $V(2,2)$ with this property is compatible. It is also true that any ordering of $V(3,2)$ with zero first or last is compatible (essentially because $\mathrm{GL}(2,2)=S_3$, so any bijection of a 2-dimensional space fixing the identity is linear. I do not know what happens for higher dimensions.

3 Groups

If A is any kind of algebraic structure, we can make similar definitions:

- $\mathrm{Aut}(A)$ is the group of automorphisms of A;
- $\mathrm{End}(A)$ is the semigroup of endomorphisms of A;
- $\mathrm{PIso}(A)$ is the inverse semigroup of isomorphisms between substructures of A.

Theorem 7 *Let A be a finite abelian group. Then $|\mathrm{End}(A)| = |\mathrm{PIso}(A)|$.*

Proof We follow the proof of the preceding theorem. We specify an element of $\mathrm{PIso}(A)$ by choosing two isomorphic subgroups of A and an isomorphism between them. We specify an element of $\mathrm{End}(A)$ by choosing a subgroup W as image, a subgroup U as kernel with $A/U \cong W$, and an isomorphism from A/U to W. Now any finite abelian group A has a dual group $A^* = \mathrm{Hom}(A,\mathbb{C}^\times)$. We have $A^* \cong A$. For any subgroup B of A, let $B^\dagger = \{f \in A^* : (\forall b \in B) bf = 1\}$; then $A^*/B^\dagger \cong B$. So the number of subgroups of A isomorphic to B is equal to the number of subgroups C with $A/C \cong B$, and the two numbers in the theorem are equal.

Problem Is it true that, if a finite group G satisfies $|\mathrm{End}(G)| = |\mathrm{PIso}(G)|$, then G is abelian?

Nik Ruskuc and I computed a few examples and found no counterexample to this assertion. We can prove something under stronger assumptions. If X and A are structures, we define $s_A(X)$ and $q_A(X)$ to be the numbers of substructures and quotient structures, respectively, of X which are isomorphic to A. We say that X satisfies *SQ-duality* if $s_A(X) = q_A(X)$ for every substructure A of X; in other words, for any structure A, either $s_A(X) = 0$ or $s_A(X) = q_A(X)$. Clearly the argument above shows that, if X satisfies SQ-duality, then $|\mathrm{End}(X)| = |\mathrm{PIso}(X)|$.

Theorem 8 *A finite group satisfying SQ-duality is abelian.*

Proof Let G be any finite group. In this proof, summations are always over the isomorphism types of groups A embeddable in G, that is, for which $s_A(G) \neq 0$.

Now $\sum s_A(G)$ is the number of subgroups of G, while $\sum q_A(G)$ is the number of normal subgroups with quotient embeddable in G. So equality of these two sums implies that every subgroup of G is normal and every quotient of G is embeddable in G.

If G satisfies SQ-duality, then $s_A(G) = q_A(G)$ for any group A embeddable in G, so indeed the two sums of the previous paragraph are equal. This implies in particular that G is *Hamiltonian*, that is, every subgroup of G is normal. A Hamiltonian group which is not abelian has the form $G = Q_8 \times (C_2)^r \times B$, where C_2 and Q_8 are the cyclic group of order 2 and quaternion group of order 8 respectively, and B is an abelian group of odd order. But this group has a quotient $(C_2)^{r+2}$ which is not a subgroup, so does not satisfy SQ-duality. The result is proved.