C50 Enumerative & Asymptotic Combinatorics

Notes 4 Spring 2003

Much of the enumerative combinatorics of sets and functions can be generalised in a manner which, at first sight, seems a bit unmotivated. In this chapter, we develop a small amount of this large body of theory.

Motivation

We can look at q-analogues in several ways:

- The q-analogues are, typically, formulae which tend to the classical ones as $q \to 1$. Most basic is the fact that

$$\lim_{q\to 1} \frac{q^a - 1}{q - 1} = a$$

  for any real number a (this is immediate from l'Hôpital's rule).

- There is a formal similarity between statements about subsets of a set and subspaces of a vector space, with cardinality replaced by dimension. For example, the inclusion-exclusion rule

$$|U \cup V| + |U \cap V| = |U| + |V|$$

  for sets becomes

$$\dim(U + V) + \dim(U \cap V) = \dim(U) + \dim(V)$$

  for vector spaces. Now, if the underlying field has q elements, then the number of 1-dimensional subspaces of an n-dimensional vector space is $(q^n - 1)/(q - 1)$, which is exactly the q-analogue of n.

- The analogy can be interpreted at a much higher level, in the language of *braided categories*. I will not pursue this here. You can read more in various papers of Shahn Majid, for example Braided Groups, *J. Pure Appl. Algebra* **86** (1993), 187–221; Free braided differential calculus, braided binomial theorem and the braided exponential map, *J. Math. Phys.* **34** (1993), 4843–4856.

In connection with the second interpretation, note the theorem of Galois:

Theorem 1 *The cardinality of any finite field is a prime power. Moreover, for any prime power q, there is a unique field with q elements, up to isomorphism.*

To commemorate Galois, finite fields are called *Galois fields*, and the field with q elements is denoted by $\mathrm{GF}(q)$.

Definition The *Gaussian coefficient,* or *q-binomial coefficient,* $\begin{bmatrix} n \\ k \end{bmatrix}_q$, where n and k are natural numbers and q a real number different from 1, is defined by

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

Proposition 2 *(a)* $\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}$.

(b) If q is a prime power, then the number of k-dimensional subspaces of an n-dimensional vector space over $\mathrm{GF}(q)$ *is equal to* $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Proof The first assertion is almost immediate from $\lim_{q\to 1}(q^n-1)/(q-1) = n$.

For the second, note that the number of choices of k linearly independent vectors in $\mathrm{GF}(q)^n$ is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{k-1}),$$

since the ith vector must be chosen outside the span of its predecessors. Any such choice is the basis of a unique k-dimensional subspace. Putting $n = k$, we see that the number of bases of a k-dimensional space is

$$(q^k-1)(q^k-q)\cdots(q^k-q^{k-1}).$$

Dividing and cancelling powers of q gives the result.

The q-binomial theorem

The q-binomial coefficients satisfy an analogue of the recurrence relation for binomial coefficients.

Proposition 3 $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = \begin{bmatrix} n \\ n \end{bmatrix}_q = 1, \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ *for* $0 < k < n$*.*

Proof This comes straight from the definition. Suppose that $0 < k < n$. Then

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q &= \left(\frac{q^n - 1}{q^k - 1} - 1 \right) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \\ &= q^k \left(\frac{q^{n-k} - 1}{q^k - 1} \right) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \\ &= q^k \begin{bmatrix} n \\ k-1 \end{bmatrix}_q . \end{aligned}$$

The array of Gaussian coefficients has the same symmetry as that of binomial coefficients. From this we can deduce another recurrence relation.

Proposition 4 *(a) For* $0 \leq k \leq n$*,*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q .$$

(b) For $0 < k < n$*,*

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

Proof (a) is immediate from the definition. For (b),

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \begin{bmatrix} n \\ n-k \end{bmatrix}_q \\ &= \begin{bmatrix} n-1 \\ n-k-1 \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ n-k \end{bmatrix}_q \\ &= \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q . \end{aligned}$$

We come now to the q-analogue of the binomial theorem, which states the following.

Theorem 5 *For a positive integer n, a real number $q \neq 1$, and an indeterminate z, we have*

$$\prod_{i=1}^{n}(1+q^{i-1}z) = \sum_{k=0}^{n} q^{k(k-1)/2} z^k \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

Proof The proof is by induction on n; starting the induction at $n = 1$ is trivial. Suppose that the result is true for $n-1$. For the inductive step, we must compute

$$\left(\sum_{k=0}^{n-1} q^{k(k-1)/2} z^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q\right)\left(1+q^{n-1}z\right).$$

The coefficient of z^k in this expression is

$$\begin{aligned}
& q^{k(k-1)/2} \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{(k-1)(k-2)/2+n-1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \\
= \;& q^{k(k-1)/2} \left(\begin{bmatrix} n-1 \\ k \end{bmatrix}_q + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q \right) \\
= \;& q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q
\end{aligned}$$

by Proposition 4(b).

Elementary symmetric functions

In this section we touch briefly on the theory of elementary symmetric functions.

Let $x_1, \ldots, x_n$ be n indeterminates. For $1 \leq k \leq n$, the kth *elementary symmetric function* $e_k(x_1, \ldots, x_n)$ is the sum of all monomials which can be formed by multiplying together k *distinct* indeterminates. Thus, e_k has $\binom{n}{k}$ terms, and

$$e_k(1,1,\ldots,1) = \binom{n}{k}.$$

For example, if $n = 3$, the elementary symmetric functions are

$$e_1 = x_1 + x_2 + x_3, \quad e_2 = x_1x_2 + x_2x_3 + x_3x_1, \quad e_3 = x_1x_2x_3.$$

We adopt the convention that $e_0 = 1$.

Newton observed that the coefficients of a polynomial of degree n are the elementary symmetric functions of its roots, with appropriate signs:

Proposition 6 $\prod_{i=1}^{n}(z-x_i) = \sum_{k=0}^{n}(-1)^k e_k(x_1,\ldots,x_n)z^{n-k}$.

Consider the generating function for the e_k:

$$E(z) = \sum_{k=0}^{n} e_k(x_1,\ldots,x_n)z^k.$$

A slight rewriting of Newton's Theorem shows that

$$E(z) = \prod_{i=1}^{n}(1+x_i z).$$

Hence the binomial theorem and its q-analogue give the following specialisations:

Proposition 7 *(a) If $x_1 = \ldots = x_n = 1$, then*

$$E(z) = (1+z)^n = \sum_{k=0}^{n}\binom{n}{k}z^k,$$

so

$$e_k(1,1,\ldots,1) = \binom{n}{k}.$$

(b) If $x_i = q^{i-1}$ for $i = 1,\ldots,n$, then

$$E(z) = \prod_{i=1}^{n}(1+q^{i-1}z) = \sum_{k=0}^{n} q^{k(k-1)/2}z^k \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

so

$$e_k(1,q,\ldots,q^{n-1}) = q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix}_q.$$

Partitions and permutations

The number of permutations of an n-set is $n!$. The linear analogue of this is the number of linear isomorphisms from an n-dimensional vector space to itself; this is equal to the number of choices of basis for the n-dimensional space, which is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

These linear maps form a group, the *general linear group* $\mathrm{GL}(n,q)$.

Using the q-binomial theorem, we can transform this multiplicative formula into an additive formula:

Proposition 8

$$|\mathrm{GL}(n,q)| = (-1)^n q^{n(n-1)/2} \sum_{i=0}^{n} (-1)^k q^{k(k+1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

Proof We have

$$|\mathrm{GL}(n,q)| = (-1)^n q^{n(n-1)/2} \prod_{i=1}^{n} (1-q^i),$$

and the right-hand side is obtained by substituting $z = -q$ in the q-binomial theorem.

The total number of $n \times n$ matrices is q^{n^2}, so the probability that a random matrix is invertible is

$$p_n(q) = \prod_{i=1}^{n} (1-q^{-i}).$$

As $n \to \infty$, we have

$$p_n(q) \to p(q) = \prod_{i \geq 1} (1-q^{-i}).$$

According to Euler's Pentagonal Numbers Theorem, we have

$$p(q) = \sum_{k \in \mathbb{Z}} (-1)^k q^{-k(3k-1)/2} = 1 - q^{-1} - q^{-2} + q^{-5} + q^{-7} - q^{-12} - \cdots$$

So, for example, $p(2) = 0.2887\ldots$ is the limiting probability that a large random matrix over $\mathrm{GF}(2)$ is invertible.

What is the q-analogue of the Stirling number $S(n,k)$, the number of partitions of an n-set into k parts? This is a philosophical, not a mathematical question; I argue that the q-analogue is the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

The number of surjective maps from an n-set to a k-set is $k!S(n,k)$, since the preimages of the points in the k-set form a partition of the n-set whose k parts can be mapped to the k-set in any order. The q-analogue is the number of surjective linear maps from an n-space V to a k-space W. Such a map is determined by its kernel U, an $(n-k)$-dimensional subspace of V, and a linear isomorphism from V/U to W. So the analogue of $S(n,k)$ is the number of choices of U, which is

$$\begin{bmatrix} n \\ n-k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

Irreducible polynomials

Though it is not really a q-analogue of a classical result, the following theorem comes up in various places. Recall that a polynomial of degree n is *monic* if the coefficient of x^n is equal to 1.

Theorem 9 *The number* $f_q(n)$ *of monic irreducible polynomials of degree n over* $\mathrm{GF}(q)$ *satisfies*

$$\sum_{k|n} k f_q(k) = q^n.$$

Proof We give two proofs, one depending on some algebra, and the other a rather nice exercise in manipulating formal power series.

First proof: We use the fact that the roots of an irreducible polynomial of degree k over $\mathrm{GF}(q)$ lie in the unique field $\mathrm{GF}(q^k)$ of degree k over $\mathrm{GF}(q)$. Moreover, $\mathrm{GF}(q^k) \subseteq \mathrm{GF}(q^n)$ if and only if $k \mid n$; and every element of $\mathrm{GF}(q^n)$ generates some subfield over $\mathrm{GF}(q)$, which has the form $\mathrm{GF}(q^k)$ for some k dividing n.

Now each of the q^n elements of $\mathrm{GF}(q^n$ satisfies a unique minimal polynomial. of degree k for some k; and every irreducible polynomial arises in this way, and has k distinct roots. So the result holds.

Second proof: All the algebra we use in this proof is that each monic polynomial of degree n can be factorised uniquely into monic irreducible factors. If the number of monic irreducibles of degree k is m_k, then we obtain all monic polynomials of degree n by the following procedure:

- Express $n = \sum a_k k$, where a_k are non-negative integers;
- Choose a_k monic irreducibles of degree k from the set of all m_k such, with repetitions allowed and order not important;
- Multiply the chosen polynomials together.

Altogether there are q^n monic polynomials $x^n + c_1 x^{n-1} + \cdots + c_n$ of degree n, since there are q choices for each of the n coefficients. Hence

$$q^n = \sum \prod_k \binom{m_k + a_k - 1}{a_k}, \tag{1}$$

where the sum is over all sequences $a_1, a_2, \ldots$ of natural numbers which satisfy $\sum k a_k = n$.

Multiplying by x^n and summing over n, we get

$$\begin{aligned}
\frac{1}{1-qx} &= \sum_{n\ge 0} q^n x^n \\
&= \sum_{a_1,a_2,\ldots} \prod_{k\ge 1} \binom{m_k+a_k-1}{a_k} x^{ka_k} \\
&= \prod_{k\ge 1} \sum_{a\ge 0} \binom{m_k+a-1}{a} (x^k)^a \\
&= \prod_{k\ge 1} (1-x^k)^{-m_k}.
\end{aligned}$$

Here the manipulations are similar to those for the sum of cycle indices in Chapter 2; we use the fact that the number of choices of a things from a set of m, with repetition allowed and order unimportant, is $\binom{m+a-1}{a}$, and in the fourth line we invoke the Binomial Theorem with negative exponent.

Taking logarithms of both sides, we obtain

$$\begin{aligned}
\sum_{n\ge 1} \frac{q^n x^n}{n} &= -\log(1-qx) \\
&= \sum_{k\ge 1} -m_k \log(1-x^k) \\
&= \sum_{k\ge 1} m_k \sum_{r\ge 1} \frac{x^{kr}}{r}.
\end{aligned}$$

The coefficient of x^n in the last expression is the sum, over all divisors k of n, of $m_k/r = km_k/n$. This must be equal to the coefficient on the left, which is q^n/n. We conclude that

$$q^n = \sum_{k\mid n} km_k, \tag{2}$$

as required.

Note how the very complicated recurrence relation (1) for the numbers m_k changes into the much simpler recurrence relation (2) after taking logarithms!

We will see how to solve such a recurrence in the section on Möbius inversion.