MT5821 Advanced Combinatorics

6 Gaussian coefficients

The q-anaolgue of a combinatorial formula is, loosely speaking, a formula involving a parameter q, which tends to the original formula as $q \to 1$. However, this is much too vague to be a definition, and it turns out that there are some very specific q-analogues which crop up in several different fields. Most important of these are the Gaussian, or q-binomial, coefficients, which we discuss in this chapter. Among other places, they come up in the following areas:

- Combinatorics of vector spaces over finite fields. It turns out that there are close analogies between sets and subsets, on one hand, and vector spaces and subspaces, on the other. The counting formulae replace the binomial coefficients by their q-analogues.
- Lattice paths. We know that the number of lattice paths from $(0,0)$ to (m,n) (using only northward and eastward steps) is $\binom{m+n}{n}$. To count these paths by the area under them, we introduce a new variable q to give a generating function, and the formula becomes the q-analogue of the binomial coefficient.
- Non-commutative geometry. I will not give a detailed account of this, but note a couple of occurrences. The simplest to describe is the binomial theorem for indeterminates x, y which satisfy $yx = qxy$; the binomial coefficients in the expansion are replaced by their q-analogues.

There are several further applications of the q-binomial coefficients, among them quantum calculus and braided categories. I will not discuss these, but there is a very accessible book on quantum calculus if you are interested: V. Kac and P. Cheung, *Quantum Calculus*, Springer, New York, 2002.

6.1 The definition

Let n and k be non-negative integers. The *Gaussian* or *q-binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined to be

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

In other words, we take the formula for the binomial coefficient, and replace each factor m in either numerator or denominator by q^m-1.

For example,

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{(q^4-1)(q^3-1)}{(q^2-1)(q-1)} = (q^2+1)(q^2+q+1),$$

a polynomial of degree 4 in q. Putting $q=1$, we obtain $2\cdot 3 = 6$, which is equal to $\binom{4}{2}$.

Proposition 6.1

$$\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}.$$

Proof By L'Hôpital's Rule, we have

$$\lim_{q\to 1} \frac{q^a-1}{q^b-1} = \lim_{q\to 1} \frac{aq^{a-1}}{bq^{b-1}} = \frac{a}{b}.$$

Now break the fractional expression giving the Gaussian coefficient into the product of k fractions, of which the ith tends to $(n-i+1)/(k-i+1)$ as $q\to 1$. The result follows.

6.2 Vector spaces over finite fields

The number of elements in a finite field is necessarily a prime power, and there is a unique field (up to isomorphism) of any given prime power order. The field with q elements is denoted by $\mathrm{GF}(q)$, or sometimes $\mathbb{F}_q$.

From elementary linear algebra, we know that an n-dimensional vector space V over GF(q) has a basis $v_1, \ldots, v_n$ such that every vector v has a unique expression as a linear combination of basis vectors:

$$v = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n, \qquad c_i \in \mathrm{GF}(q).$$

So, as usual, V can be identified with the space $GF(q)^n$ of all n-tuples of elements of GF(q), with coordinatewise operations. In particular, we see:

Proposition 6.2 *If V is an n-dimensional vector space over* GF(q)*, then $|V| = q^n$.*

Now the connection with Gaussian coefficients is the following:

Theorem 6.3 *The number of k-dimensional subspaces of an n-dimensional vector space over* GF(q) *is* $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Proof We specify a k-dimensional subspace by giving a basis, a linearly independent k-tuple $(v_1, \ldots, v_k)$ of vectors in V. The number of choices

- for v_1 is $q^n - 1$ (any vector except 0);
- for v_2 is $q^n - q$ (any vector except one of the q multiples of v_1);
- for v_3 is $q^n - q^2$ (any vector except one of the q^2 linear combinations of v_1 and v_2);

and so on; the total number of choices is

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

However, we have over-counted, since a given k-dimensional subspace has many bases. How many? The number is found from the same formula using k instead of n, since we are working within a k-dimensional space.

So the number of k-dimensional subspaces is

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

Cancelling powers of q, this reduces to the formula for the Gaussian coefficient.

This result has another counting interpretation. Recall that a $k \times n$ matrix A over a field F is in *reduced echelon form* if

- if a row is not identically zero, the first non-zero element in it is 1;
- the "leading ones" in the non-zero rows occur further to the right as we go down the matrix;
- all the other elements in the column of a leading one are zero.

Now standard linear algebra shows that any matrix can be put into reduced echelon form by elementary row operations, which do not change the row space of the matrix. So any k-dimensional subspace of F^n has a basis whose vectors are the rows of a matrix in reduced echelon form. Moreover, it is easy to see that the reduced echelon basis of a given subspace is unique. So:

Proposition 6.4 *The number of $k \times n$ matrices over* GF(q) *which have no zero rows and are in reduced echelon form is* $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

The definition of "reduced echelon" does not depend on properties of fields; any alphabet containing distinguished elements called 0 and 1 will do. So we have a counting interpretation of the Gaussian coefficients for arbitrary positive integers $q > 1$.

Example For $n = 4$ and $k = 2$, the matrices in reduced echelon form are shown. $*$ can be any element of the field. Beside each matrix is the number of matrices of this form over GF(q).

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix} \quad q^4$$

$$\begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix} \quad q^3$$

$$\begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad q^2$$

$$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix} \quad q^2$$

$$\begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad q$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad 1$$

We find, as before, that $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = (q^2+1)(q^2+q+1)$.

6.3 Relations between Gaussian coefficients

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

Proposition 6.5 $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = \begin{bmatrix} n \\ n \end{bmatrix}_q = 1, \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ *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

Proposition 6.6

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

The proof is an exercise from the formula. Note that, in the vector space interpretation, we have a different way to see this. Given an n-dimensional vector space V over GF(q), it has a *dual space* V^*, the space of linear maps from V to GF(q). Now any k-dimensional subspace of V has an $(n-k)$-dimensional *annihilator* in V^*, and the correspondence between k-dimensional subspaces of V and $(n-k)$-dimensional subspaces of V^* is bijective.

From this we can deduce another recurrence relation.

Proposition 6.7 $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = \begin{bmatrix} n \\ n \end{bmatrix}_q = 1, \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q = q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ *for* $0 < k < n$.

Proof

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

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

Theorem 6.8 *For a positive integer n, a real number $q \neq 1$, and an indeterminate x, we have*

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

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

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

The coefficient of x^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 6.7.

6.4 Lattice paths

We consider lattice paths from the origin to the point (m,n), where m and n are non-negative integers, and the allowable steps are east and north. The number of paths is $\binom{m+n}{m}$, since we have to take $m+n$ steps altogether, of which m must be easterly and n northerly.

For each such path p, there is a certain area $A(p)$ enclosed between the path, the X-axis, and the line $x = m$. Figure 1 shows the six paths for $m = n = 2$ and the area enclosed in each case.

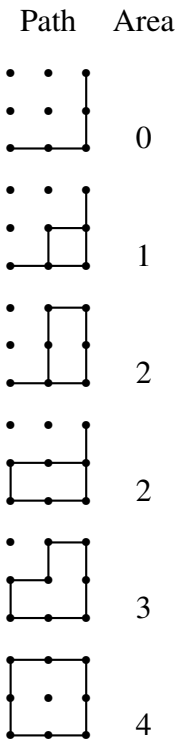

Figure 1: Lattice paths

If we take a generating function in the variable q for these areas, that is, a path with area A contributes q^A to the sum, we obtain

$$1+q+2q^2+q^3+q^4 = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q.$$

This is quite general:

Theorem 6.9 *Let $\mathscr{P}$ be the set of lattice paths from $(0,0)$ to (m,n) using northerly and easterly steps only. For $p \in \mathscr{P}$, let $A(p)$ be the area enclosed by p, the X-axis and the line $x = m$. Then*

$$\sum_{p \in \mathscr{P}} q^{A(p)} = \begin{bmatrix} m+n \\ m \end{bmatrix}_q.$$

Proof Call the left-hand side $F(m,n)$. It is clear that $F(0,n) = F(m,0) = 0$. Now consider $F(m,n)$. There are two cases:

- If the last step on the path p is northerly, then it is a path from $(0,0)$ to $(m,n-1)$ followed by a northerly step, and the last step doesn't change the area.
- If the last step is easterly, then p is a path from $(0,0)$ to $(m-1,n)$ followed by an easterly step, which adds n to the area.

So

$$F(m,n) = F(m,n-1) + q^n F(m-1,n).$$

Now a simple induction using Proposition 6.5 gives the result.

Exercises

6.1. Show that the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is a polynomial in q with degree $k(n-k)$.

6.2. Use the interpretation in terms of matrices in reduced echelon form to show the recurrence relation of Proposition 6.5.

6.3. Show that the polynomial in the first problem has coefficients which are symmetric, that is, if

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{i=0}^{k(n-k)} a_i q^i,$$

then $a_i = a_{k(n-k)-i}$.

6.4. A matrix is said to be in *echelon form* if it satisfies the first two of the three conditions for reduced echelon form.

Show that, if q is an integer greater than 2, the right-hand side of the q-binomial theorem with $x = 1$ counts the number of $n \times n$ matrices in echelon form.

6.5. Let x and y be elements of an algebra, which satisfy $yx = qxy$. Prove that

$$(x+y)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q x^{n-k} y^k.$$

6.6. Let X be the set of 1-dimensional subspaces of an n-dimensional vector space V over GF(q), where $n \geq 3$. For any 2-dimensional subspace W of V, let $B(W)$ be the set of 1-dimensional subspaces contained in W, and let $\mathscr{B}$ be the collection of all blocks or subsets of X arising in this way. Prove that $(X, \mathscr{B})$ is a $(2, q+1, (q^n-1)/(q-1))$ Steiner system. (This system is known as the $(n-1)$-dimensional *projective space* over GF(q).)