Lecture 5: Binomial identities.

Aims:
- To give some analogous $q$-binomial identities.
- To present a combinatorial application of the $q$-calculus.

5.1. Binomial Identities. Last lecture we proved two versions of $q$-Pascal’s rule:

**Proposition 5.1.** The following $q$-binomial identities hold

\[
\binom{n}{j} = \binom{n-1}{j-1} + q^j \binom{n-1}{j},
\]

(5.1)

\[
\binom{n}{j} = q^{n-j} \binom{n-1}{j-1} + \binom{n-1}{j}
\]

(5.2)

These are very useful identities. The first consequence we show is that we may regard each $q$-binomial as an element of $\mathbb{Z}[q]$.

**Corollary 5.2.** Each $q$-binomial coefficient,

\[
\binom{n}{j} = \frac{[n]!}{[j]![n-j]!},
\]

is a monic polynomial in $q$ of degree $j(n-j)$.

**Proof.** Let us proceed by induction on $n$. The first step is easy because

\[
\binom{1}{0} = \binom{1}{1} = 1.
\]

Now let us fix an integer, $n$, and assume that for each $k$ the $q$-binomial $\binom{n}{k}$ is an element of $\mathbb{Z}[q]$, then by the closure of $\mathbb{Z}[q]$ under addition and multiplication, so is

\[
\binom{n+1}{j} = \binom{n}{j} + q^j \binom{n}{j-1}.
\]

This shows each $q$-binomial is an element of $\mathbb{Z}[q]$, as required.

To prove the degree is $j(n-j)$, notice that, by definition

\[
\frac{[n]!}{[j]![n-j]!} = \frac{(q^n - 1)(q^{n-1} - 1)\ldots(q^{n-j+1} - 1)}{(q^j - 1)(q^{j-1} - 1)\ldots(q - 1)}.
\]
then the first term in the expansion around \( q = \infty \) is
\[
= q^{n+(n-1)+\ldots+(n-j+1)} + O(other)
\]
\[
= q^{j(2n-j+1) - (j-1)/2} + O(other),
\]
\[
= q^{j(2n-2j)/2} + O(other)
\]
\[
= q^{j(n-j)} + O(other)
\]
which proves the degree. \( \square \)

While the theorem is ridiculously easy to prove, actually finding these polynomials can be a little more cumbersome. So in general,

\[
\binom{n}{j} = a_0 + a_1 q + \ldots a_j(n-j)q^{j(n-j)}
\]

for some collection of integers, \( a_i \).

**Example 5.3.** Let us consider a simple example

\[
\begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} + q^3 \begin{pmatrix} 4 \\ 3 \end{pmatrix}
\]

\[
= \begin{pmatrix} 3 \\ 2 \end{pmatrix} + q^2 \begin{pmatrix} 3 \\ 2 \end{pmatrix} + q^3 \begin{pmatrix} 3 \\ 2 \end{pmatrix} + q^6
\]

\[
= 1 + q + (q^2 + q^3) \left( \begin{pmatrix} 2 \\ 1 \end{pmatrix} + q \right) + q^6
\]

\[
= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6.
\]

One thing this example suggests is that the coefficients (as a function of \( q \)) are symmetric.

**Proposition 5.4.** Given the \( a_i \) from (5.3), they satisfy

\[
a_i = a_j(n-j)-i
\]

**Proof.** By definition, the left hand side of (5.3) is

\[
\frac{(1-q)(1-q^2)\ldots(1-q^{n-1})(1-q^n)}{(1-q)(1-q^2)\ldots(1-q^j)(1-q^2)\ldots(1-q^{n-j})}.
\]

If we replace, in this statement, \( q \) with \( 1/q \), and multiply by \( q^{j(n-j)} \), it is easy to see this statement remains unchanged. The right hand side is

\[
a_{j(n-j)} + a_{j(n-j)+1}q + \ldots + a_0q^{j(n-j)}
\]
giving the required identity. \( \square \)

**5.2. \( q \)-Vandermonde identity.** Recall the Vandermonde identity, which can be derived from the two forms of the expansion of \((1+x)^{m+n}\), as we see

\[
(1+x)^{m+n} = (1+x)^m(1+x)^n \sum_k \binom{m+n}{k} x^k
\]

\[
= \sum_i \sum_j \binom{m}{i} \binom{n}{j} x^{i+j},
\]
so by comparing coefficients of $x^k$ we have

$$\binom{m+n}{k} = \sum_j \binom{m}{k-j} \binom{n}{j},$$

which we wish to find the $q$-analogue of this result.

\begin{align*}
\begin{array}{ccccccc}
1 & 1 & 1 & 1 & 3 & 3 & 1 \\
1 & 5 & 4 & 6 & 4 & 20 & 15 & 7 & 1 \\
1 & 6 & 15 & 20 & 15 & 6 & 1 \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \\
\end{array}
\end{align*}

\begin{align*}
\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} = \binom{7}{4} \\
1 + 4 \times 3 + 6 \times 3 + 4 \times 1 = 35
\end{align*}

In lecture 3, we presented the following identity

$$(x - a)^{m+n} = (x - a)^m (x - q^m a)^n,$$

which we may use, in conjunction with the special version of Gauss’s binomial identity from last lecture,

$$(1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k q^{k(k-1)/2},$$

to obtain a $q$-version of the above identity.

**Proposition 5.5.** The $q$-Chu-Vandermonde identity is stated as

$$\binom{m+n}{k} = \sum_j \binom{m}{k-j} \binom{n}{j} q^{j(m+j-k)}$$

**Proof.** The decomposition of $(1 + x)^{m+n}$, by using the above, is

$$(1 + x)^{m+n} = (1 + x)^m (1 + q^m x)^n.$$  

The left hand side, by Gauss’s binomial formula, is

$$(1 + x)^{m+n} = \sum_k \binom{m+n}{k} x^k q^{k(k-1)/2}.$$  

Similarly, the left hand side may be expressed as

$$= \sum_i \binom{m}{i} x^i q^{i(i-1)/2} (1 + x q^m)^n_q$$

$$= \sum_i \sum_j \binom{m}{i} \binom{n}{j} x^{i+j} q^{m i j} q^{i(i-1)/2} q^{j(j-1)/2},$$

comparing the coefficient of $x^k$ on the left, and by letting $i = k - j$, we can compare the coefficient of $x^k$ on the right hand side to give

$$\binom{m+n}{k} q^{k(k-1)/2} = \sum_j \binom{m}{k-j} \binom{n}{j} q^{m j} q^{(k-j)(k-j-1)/2} q^{j(j-1)/2},$$
shifting powers of $q$ to the right hand side, we find that the exponent of $q$ is
\[ mj + \frac{(k-j)(k-j-1)}{2} + \frac{j(j-1)}{2} - \frac{k(k-1)}{2} \]
\[ = mj + \frac{k^2 - kj + j^2}{2} - \frac{k + j + j^2 - j}{2} + \frac{k^2}{2} + \frac{j^2}{2} \]
\[ = mj + j^2 - jk \]
\[ = j(m + j - k). \]
This means that
\[ \left[ \begin{array}{c} m + n \\ k \\ \end{array} \right] = \sum_j \left[ \begin{array}{c} m \\ k - j \\ \end{array} \right] \left[ \begin{array}{c} n \\ j \\ \end{array} \right] q^{j(m+j-k)}, \]
as required.

5.3. Combinatorics with the $q$-calculus. One last theorem (for today) is related to the way in which these binomials may be seen to count certain things over finite fields. This relates our work to combinatorics.

**Theorem 5.6.** Let $q$ be the order of a finite field, $F_q$ ($q$ is a prime power), then
\[ \left[ \begin{array}{c} n \\ j \\ \end{array} \right] = \text{The number of } j\text{-dimensional subspaces of } F_q^n. \]

**Proof.** The case in which $j = 0$ or $j = n$ is too trivial to mention. Firstly, $|F_q| = q$, hence, if we think of a standard canonical basis, $e_1, e_2, \ldots, e_n$, any element of $F_q^n$ is given by
\[ v = a_1 e_1 + \ldots + a_n e_n, \]
which is often denoted by the $n$-tuple $(a_1, \ldots, a_n)$. The number of choices for each $a_i$ is $q$ making $q^n$ total elements.

Every one dimensional vector sub-space is spanned by a non-zero element, making $q^n - 1$ choices. However, any linearly dependent vector also spans the subspace. I.e., \{v\} is a basis the same sub-space as \{av\} for any $a \neq 0$. There are $q - 1$ such linearly dependent, vectors making the number of 1 dimensional subspaces equal to
\[ \frac{q^n - 1}{q - 1} = \left[ \begin{array}{c} n \\ 1 \\ \end{array} \right]. \]

There are $q$ elements of this subspace.

To define a new subspace, $V_2$ from a one-dimensional subspace, $V_1$, we need to specify a non-zero element not in $V_1$. There are $q^n - q$ such elements, but we also have to divide by the total possible number of basis that spans $V_2$. We have $q^2 - 1$ elements to choose from to form our first basis vector and $q^2 - q$ elements to choose from to make our second basis vector, making $(q^2 - 1)(q^2 - q)$ in total. This means the number of two dimensional subspaces is
\[ \frac{(q^n - 1)(q^n - q)}{(q^2 - 1)(q^2 - q)} = \frac{(q^n - 1)(q^{n-1} - 1)}{(q^2 - 1)(q - 1)}. \]
We could go on, to $V_3$, but in general, we have that the number of $j$-dimensional subspaces is

$$\frac{(q^n - 1)(q^n - q)\ldots(q^n - q^{j-1})}{(q^j - 1)(q^{j-1} - 1)\ldots(q - 1)},$$

$$= \frac{(q^n - 1)(q^{n-1} - 1)\ldots(q^{n-j} - 1)}{(q^j - 1)(q^{j-1} - 1)\ldots(q - 1)},$$

$$= \frac{q^n - 1}{q-1} \frac{q^n - 1}{q-1} \ldots \frac{q^{n-j} - 1}{q-1},$$

$$= \frac{[n][n-1]\ldots[n-j+1]}{[j]!},$$

$$= \frac{[n]!}{[j]![n-j]!} = \binom{n}{j}.$$ 

This concludes the proof. □