q-combinatorics

February 7, 2019

1 q-binomial coefficients

Definition. For natural numbers n, k,the *q-binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ (or just $\begin{bmatrix} n \\ k \end{bmatrix}$ if there no ambiguity on q) is defined as the following rational function of the variable q:

$$\frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)\cdot(q^{n-k}-1)(q^{n-k-1}-1)\cdots(q-1)}. \tag{1.1}$$

For $n = 0$, $k = 0$, or $n = k$, we interpret the corresponding products 1, as the value of the empty product. If we exclude certain roots of unity from the domain of q, (1.1) is equal to

$$\begin{aligned} &\frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)\cdot 1} \\ &= \frac{(q^{n-1}+\ldots+q+1)\cdots(q^2+q+1)(q+1)\cdot 1}{(q^{k-1}+\ldots+q+1)\cdots(q^2+q+1)(q+1)\cdot 1(q^{n-k-1}+\ldots+q+1)\cdots(q^2+q+1)(q+1)\cdot 1}. \end{aligned} \tag{1.2}$$

As the notation starts to be overwhelming, we introduce to *q-analogue of the positive integer n*, denoted by $[n]$ or $[n]_q$, as $q^{n-1}+\ldots+q+1$; and the *q-analogue of the factorial of the positive integer n*, denoted by $[n]!$ or $[n]_q!$, as $[n]_q! = [1]_q \cdot [2]_q \cdots [n]_q$. With this additional notation, we also can say

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}, \tag{1.3}$$

when we avoid certain roots of unity with q. It is easy too see from (1.1) that

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_q = \begin{bmatrix} n \\ n \end{bmatrix}_q = 1$$

and that for every $0 \leq k \leq n$ the symmetry rule

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

holds. Furthermore, as

$$\lim_{q\to 1}[n]_q = n \text{ and } \lim_{q\to 1}[n]_q! = n!,$$

(1.3) implies that

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

This justifies using the name q-binomial coefficient. They are also called Gaussian binomial coefficients.

Claim 1 *The q-binomial coefficient is not just a rational function of q, it is actually a polynomial of q.*

We prove this by induction on n. We extend the definition of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for $k < 0$ and $k > n$ with $\begin{bmatrix} n \\ k \end{bmatrix}_q = 0$. We have $\begin{bmatrix} 0 \\ 0 \end{bmatrix}_q = 1$, and as 0 and 1 are polynomials of q, the claim holds $n = 0$. Next we observe that the familiar recurrence of binomial coefficients in the Pascal Triangle

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{1.4}$$

has its analogue for the q-binomial coefficients in the form

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{n-k+1} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q. \tag{1.5}$$

This easy to verify directly from (1.1). However, if $\begin{bmatrix} n \\ k \end{bmatrix}_q$ and $\begin{bmatrix} n \\ k-1 \end{bmatrix}_q$ are polynomials of q, then so is $\begin{bmatrix} n+1 \\ k \end{bmatrix}_q$, due to (1.5).

It is easy to compute the degree of the polynomial $\begin{bmatrix} n \\ k \end{bmatrix}_q$. There must be cancellation in the formula (1.1), as it gives a polynomial. So the degree of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ must be the difference between the degrees of the numerator and denominator in (1.1). We have

$$deg\left(\begin{bmatrix} n \\ k \end{bmatrix}_q\right) = \binom{n+1}{2} - \binom{k+1}{2} - \binom{n-k+1}{2} = k(n-k).$$

Therefore can write

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\alpha=0}^{k(n-k)} c_{n,k,\alpha} q^{\alpha}. \tag{1.6}$$

The coefficients satisfy an unexpected new symmetry rule:

$$c_{n,k,\alpha} = c_{n,k,k(n-k)-\alpha}. \tag{1.7}$$

The reason is the following. For any polynomial $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, we have $x^n p(\frac{1}{x}) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$. Therefore, the coefficient sequence reads from top down the same way as from bottom up, if and only if $p(x) = x^n p(\frac{1}{x})$ is an identity. It is easy to see directly from (1.1) that the required identity

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

holds.

Definition A sequence is called *unimodal*, if it is increasing up to a point, and then turns decreasing. Many combinatorial sequences are unimodal, like $\binom{n}{k}$ or $S(n,k)$ for any fixed n.

Sylvester proved that $c_{n,k,\alpha}$ is unimodal for any fixed n and k using invariant theory. It took a century to find a combinatorial proof to this fact. A combinatorial proof needs counting interpretation of these numbers and then some injections. A combinatorial interpretation is the following:

Claim 2 *$c_{n,k,\alpha}$ is the number of lattice walks from $(0,0)$ to $(k, n-k)$ (using the usual horizontal and vertical steps of unit length) such that the area between the walk and the x axis is exactly α.*

We will show this from the following more general theorem. Let us be given an ordered finite alphabet like $A < B < C < ... < Z$. We define the number of inversions in a word as the number of ordered pairs of letters that stand in the wrong order. Two copies of the same letter do not contribute to this count. For example, LEECH has 6 inversions, as L contributes 4 one for each of E,E,C,H, both E contributes one more because of C, and finally CH makes no contribution.

Theorem 1 *Let us be given an ordered k-letter alphabet $x_1 < x_2 < \cdots < x_k$ and n_i copies of the letter x_i for $i = 1, 2, ..., k$. Let $w_m(n_1, ..., n_k)$ denote the number of words using all of these letters and having m inversions. Then*

$$\sum_m w_m(n_1, ..., n_k) q^m = \frac{[n_1 + n_2 + \ldots + n_k]_q!}{[n_1]_q! [n_2]_q! \cdots [n_k]_q!}. \tag{1.8}$$

The term on the RHS of (1.8) is called a *q-multinomial coefficient,* and for $k = 2$ it specializes to a q-binomial coefficient.

Corollary 2 *Given $n_1, ..., n_k$, the q-multinomial coefficient $\frac{[n_1+n_2+...+n_k]_q!}{[n_1]_q![n_2]_q!\cdots[n_k]_q!}$ is a polynomial of q. In particular, for $k = 2$, the q-binomial coefficient is a polynomial of q, proving Claim 1, without the use of the identity (1.3).*

Now we are in the position to derive the combinatorial interpretation of $c_{n,k,\alpha}$ in Claim 2. Consider a 2-letter alphabet $X < Y$, k copies of X and $n - k$ copies of Y. The words that one can build of these letters are in one-to-one correspondence with the lattice walks $(0,0)$ to $(k, n-k)$, if X indicates a horizontal step and Y indicates a vertical step, and we read the word left-to-right to find out the order of steps. Observe that the area under the lattice walk is exactly the number of inversions in the corresponding word. Indeed, look at any particular horizontal step. The total area is the sum of areas of rectangles whose top is a unit horizontal step. What is the height of such a rectangle? Exactly the number of vertical steps before horizontal step on the top, i.e. the number of Y's that came before the current X.

Proof to Theorem 1. First observe that setting $q = 1$ in (1.8) gives back the elementary counting result that the number of words that we can make from these letters equals the multinomial coefficient $\frac{(n_1+n_2+...+n_k)!}{n_1!n_2!\cdots n_k]!}$. Recall how the proof for the number of words goes. Distinguish copies of the letter x_i with superscripts as $x_i^1, x_i^2, ..., x_i^{n_i}$, for $i = 1, 2, ..., k$. The number of words with the superscripted letters is $(n_1 + n_2 + \ldots + n_k)!$, as the letters are all distinct. On the other hand, starting with set of words made of these letters without superscripts, each word gives rise to $n_1!n_2!\cdots n_k!$ superscripted words, by putting on the superscripts as we like. The identity follows, as each superscripted word is constructed in a unique way. The theorem above *refines* this result by extending enumeration to an additional variable, the number of inversions. Order the superscripted copies as $x_i^1 < x_i^2 < \cdots < x_i^{n_i}$, for $i = 1, 2, ..., k$. If you consider the inversions of a superscripted word, every inversion is either already an inversion after the deletion the superscripts from the letters of the word, or is a result of an inversion between two superscripted copies of some x_i for a unique i. More formally:

Case 1:

First we show the Theorem for $n_1 = n_2 = \ldots = n_k = 1$. The proof of this case goes by induction on k. For $k = 1$, (1.8) reads as 1=1 and is true. Assume that (1.8) holds for $k-1$, i.e.

$$\sum_m w_m(\underbrace{1, 1, ..., 1}_{k-1})q^m = [k-1]_q!. \tag{1.9}$$

Observe now that x_k an be inserted in a unique way into any word using the first $k-1$ letters exactly once with $0, 1, ..., k-1$ *new* inversions, in which x_k is involved, hence

$$(1 + q + \ldots + q^{k-1}) \sum_m w_m(\underbrace{1, 1, ..., 1}_{k-1})q^m = \sum_\ell w_\ell(\underbrace{1, 1, ..., 1}_{k})q^\ell.$$

As the identity $(1 + q + \ldots + q^{k-1})[k-1]_q! = [k]_q!$ holds, we completed the induction step and the proof to Case 1.

Case 2:

We have $n_i \geq 1$ for $i = 1, 2, ..., k$, i.e. no restrictions. We show (1.8) by proving

$$[n_1 + n_2 + \ldots + n_k]_q! = \left(\sum_m w_m(n_1, ..., n_k)q^m\right)[n_1]_q![n_2]_q!\cdots[n_k]_q!.$$

For the equality of two polynomials we have to point out that they are termwise equal, i.e. for ℓ,

$$coeff\left\{q^\ell\right\}[n_1 + n_2 + \ldots + n_k]_q! = coeff\left\{q^\ell\right\}\left(\sum_m w_m(n_1, ..., n_k)q^m\right)[n_1]_q![n_2]_q!\cdots[n_k]_q!.$$

This boils down to the identity

$$w_\ell(\underbrace{1, 1, \ldots, 1}_{n_1+n_2+\ldots+n_k}) = \sum_{m+j_1+\ldots+j_k=\ell} w_m(\underbrace{n_1, n_2, \ldots, n_k}_{k})w_{j_1}(\underbrace{1, 1, \ldots, 1}_{n_1})\cdots w_{j_k}(\underbrace{1, 1, \ldots, 1}_{n_k})$$

that basically tells that the number of inversions in word using superscripted letters once equals to the number of inversions in the same word between different letters (without superscript) plus the sum of inversions, for every type of letters, among superscripted copies of the same letter.

Corollary 3 *Given $n_1, ..., n_k$, the q-multinomial coefficient $\frac{[n_1+n_2+\ldots+n_k]_q!}{[n_1]_q![n_2]_q!\cdots[n_k]_q!}$ is a polynomial of q. In particular, for $k = 2$, the q-binomial coefficient is a polynomial of q, proving Claim 1, without the use of the identity (1.3).*

We continue with the q-binomial theorem. For $q = 1$ it gives back the ordinary binomial theorem.

Theorem 4 *For any n natural number,*

$$\prod_{i=1}^{n}(1+q^{i-1}x) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{k}{2}} x^k. \tag{1.10}$$

Note that for $n = 0$ the LHS is an empty product with value 1, and the RHS has a single term, a 1. The q-binomial theorem can be proved with an induction mimicking the induction proof of the binomial theorem. Here we show a useful proof technique in q-combinatorics. Set

$$f(x) = \prod_{i=1}^{n}(1+q^{i-1}x).$$

This is a 2-variable polynomial that we can rewrite as $f(x) = \sum_{k=0}^{n} a_k(q)x^k$, where $a_k = a_k(q)$ is a polynomial of q, in particular $a_0 = 1$. It is easy to see that $f(x)$ satisfies the following functional equation:

$$(1+x)f(qx) = f(x)(1+q^n x).$$

Extracting the coefficient of x^k from both sides we obtain $a_k q^k + a_{k-1}q^{k-1} = a_k + q^n a_{k-1}$. Solving this for $\frac{a_k}{a_{k-1}}$, we obtain

$$\frac{a_k}{a_{k-1}} = \frac{q^n - q^{k-1}}{q^k - 1}.$$

As $a_k = \frac{a_k}{a_{k-1}} \frac{a_{k-1}}{a_{k-2}} \cdots \frac{a_1}{a_0} a_0$, we obtain

$$a_k = \frac{q^n - q^{k-1}}{q^k - 1} \cdot \frac{q^n - q^{k-2}}{q^{k-1} - 1} \cdots \frac{q^n - 1}{q - 1} = q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

We state the infinite version of the q-binomial theorem, and leave its proof and applications to the problems section. Define

$$\begin{aligned}
(a;q)_0 &= 1; \text{ for a positive integer } n \\
(a;q)_n &= (1-a)(1-aq)\cdots(1-aq^{n-1}); \text{ and} \\
(q;q)_n &= (1-q)(1-q^2)\cdots(1-q^n); \text{ and for } |q|<1 \\
(a;q)_\infty &= \prod_{i=0}^{\infty}(1-aq^i).
\end{aligned}$$

Theorem 5 *For $|t| < 1$ and $|q| < 1$, the following equality holds:*

$$\sum_{n=0}^{\infty} \frac{(a;q)_n}{(q;q)_n} t^n = \frac{(at;q)_\infty}{(t;q)_\infty}. \tag{1.11}$$

2 Linear spaces over finite fields

Recall that for every prime power $q = p^\alpha$ there is unique field with q elements. We denote it by $GF(q)$. First observe that an n-dimensional linear space V has exactly q^n elements. Indeed, the linear space has a basis $\mathbf{b}_1, ..., \mathbf{b}_n$. The elements of V can be written in a unique way as linear combinations

$$\gamma_1 \mathbf{b}_1 + \cdots + \gamma_n \mathbf{b}_n,$$

where $\gamma_i \in GF(q)$. There are exactly q^n such linear combinations.

Theorem 6 *An n-dimensional linear space V has exactly $\begin{bmatrix} n \\ k \end{bmatrix}_q$ k-dimensional subspaces.*

First count in V the ordered s-tuples of linearly independent vectors: there are

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

of them. Indeed, selecting $< \mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_s >$ sequentially, we have $q^n - 1$ choices for $\mathbf{v}_1$, as it can be anything but the zero vector. For $\mathbf{v}_2$, we have $q^n - q$ choices, as it can be any vector but those among the q element span of $\mathbf{v}_1$. Finally, selecting $\mathbf{v}_s$, it can be anything but those in the span of the previously selected $s - 1$ linearly independent vectors.

As a special case ($n = k, s = k$) of the observation above, note that the number of ordered bases in a fixed k-dimensional subspace is $(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$. Finally observe that #(k-dimensional subspaces) $\times$ #(ordered bases in a fixed k-dimensional subspace) = #(ordered k-tuples of linearly independent vectors).

We work towards a combinatorial proof to the identity (1.5) for prime power q. We prove first a claim that we need.

Claim 3 *For A and B finite dimensional subspaces in some linear space over any field,*

$$dim(span\{A, B\}) = dim(A) + dim(B) - dim(A \cap B). \tag{2.12}$$

Assume $dim(A) = \ell$, $dim(B) = k$, and $dim(A \cap B) = m$. Take a basis $\mathbf{a}_1, ..., \mathbf{a}_m$ of $A \cap B$, and extend it to a basis $\mathbf{a}_1, ..., \mathbf{a}_m, \mathbf{a}_{m+1}, ..., \mathbf{a}_\ell$ of A and a basis $\mathbf{a}_1, ..., \mathbf{a}_m, \mathbf{b}_{m+1}, ..., \mathbf{b}_k$ of B. Clearly $span\{A, B\} = span\{\mathbf{a}_1, ..., \mathbf{a}_m, \mathbf{a}_{m+1}, ..., \mathbf{a}_\ell, \mathbf{b}_{m+1}, ..., \mathbf{b}_k\}$, and hence $dim(span\{A, B\}) \leq \ell + k - m = dim(A) + dim(B) - dim(A \cap B)$. On the other hand, we will show that the vectors $\mathbf{a}_1, ..., \mathbf{a}_m, \mathbf{a}_{m+1}, ..., \mathbf{a}_\ell, \mathbf{b}_{m+1}, ..., \mathbf{b}_k$ are linearly independent. If there were a linear dependence among these vectors, we can write it as

$$\gamma_1 \mathbf{a}_1 + ... + \gamma_m \mathbf{a}_m + \gamma_{m+1} \mathbf{a}_{m+1} + ... + \gamma_\ell \mathbf{a}_\ell = \beta_{m+1} \mathbf{b}_{m+1} + ... + \beta_k \mathbf{b}_k.$$

If both sides happen to be the 0 vector, then all γ's and β's must be zero, so the linear combination was trivial. If both sides happen to be $\mathbf{v}$ nonzero vector, then $\mathbf{v} \in A \cap B$. Hence it can be expressed with the base of $A \cap B$, so $\mathbf{v} = \alpha_1 \mathbf{a}_1 + ... + \alpha_m \mathbf{a}_m$. Therefore

$$\alpha_1 \mathbf{a}_1 + ... + \alpha_m \mathbf{a}_m = \beta_{m+1} \mathbf{b}_{m+1} + ... + \beta_k \mathbf{b}_k,$$

and as we see the basis vectors of B above, all α's and all β's are zero. Therefore all γ's are zero as well, the linear combination was trivial. End of the proof of the Claim.

Now we provide a combinatorial proof to the identity (1.5). Assume first that q is a prime power. Take a fixed n and k. Consider an $(n+1)$-dimensional linear space, V, over $GF(q)$. By the theorem above, it has $\begin{bmatrix} n+1 \\ k \end{bmatrix}_q$ k-dimensional subspaces. With a different count, we obtain the RHS of (1.5). Fix an n-dimensional subspace V' of V. Any H k-dimensional subspace of V either is a subspace of V' or not. By the claim above, $dim(V' \cap H) = k$ or $k-1$. The number of k-dimensional subspaces of V' is $\begin{bmatrix} n \\ k \end{bmatrix}_q$. So we have to count those H's for which $dim(V' \cap H) = k-1$. There are $\begin{bmatrix} n \\ k-1 \end{bmatrix}_q$ choices for $V' \cap H$. Observe the following bijective correspondence between the following sets:

$$\{(K, \mathbf{u}) : K \text{ subspace in } V',\ dim(K) = k-1, \mathbf{u} \notin V'\} \text{ and}$$

$$\{(L, \mathbf{w}) : L \text{ subspace in } V,\ \ dim(L) = k, dim(L \cap V') = k-1, \mathbf{w} \in L \setminus V'\},$$

and hence $\begin{bmatrix} n \\ k-1 \end{bmatrix}_q (q^{n+1} - q^n) = (q^k - q^{k-1}) \#\{L : dim(L) = k, dim(L \cap V') = k-1\}$. Therefore $\#\{L : dim(L) = k, dim(L \cap V') = k-1\} = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \frac{q^{n+1}-q^n}{q^k - q^{k-1}} = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q q^{n-k+1}$. Fix n and k. Note that the LHS and RHS of (1.5) are polynomials of q. (We used (1.5) identity in our first proof that the q-binomial coefficients are polynomials of q. Relying on that proof would make a circular argumeny here. However, we have an alternative proof in Corollary 3.) As the identity (1.5) holds for all values of two polynomials at prime power q's, (1.5) is a polynomial identity.

Let us be given a fixed base $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ of the linear space V. For vectors $\mathbf{u} = \sum_{i=1}^n \alpha_i \mathbf{v}_i$ and $\mathbf{w} = \sum_{i=1}^n \beta_i \mathbf{v}_i$, define the dot product

$$\mathbf{u} \cdot \mathbf{w} = \mathbf{u}^T \mathbf{w} = \mathbf{u}^T I \mathbf{w} = \sum_{i=1}^{n} \alpha_i \beta_i. \tag{2.13}$$

The dot product is a bilinear function of the two vectors. For a subspace L of V, define its *orthocomplement* by

$$L^\perp = \{\mathbf{v} \in V :\ \text{for all } \mathbf{u} \in L\ \mathbf{u} \cdot \mathbf{v} = 0\}.$$

It is easy to see that $L^\perp$ is a subspace of V as well, and that L is a subspace of $(L^\perp)^\perp$.

On the other hand, observe that $dim(L^\perp) = n - dim(L)$. Indeed, $L^\perp$ is nothing else but the solution space of a system of homogeneous linear equations, in n variables, where the rank of the coefficient matrix is $dim(L)$. (In other words, if $\mathbf{v}$ has zero dot product with every vector of a base of L, then it has zero dot product with every vector of L. Linearly independent vectors of L provide linearly independent rows of the coefficient matrix.) From here, $dim((L^\perp)^\perp) = n - (n - dim(L)) = dim(L)$. It follows that $L = (L^\perp)^\perp$. *Note that unlike in linear spaces over* $\mathbb{R}$*, in linear spaces over* $GF(p)$*, it may happen that* $L^\perp \cap L$ *has nonzero vectors, and then* $span\{L, L^\perp\} \neq V$. Note that all these arguments remain valid if we change the identity matrix I in the definition of the dot product, formula (2.13), to any non-singular $n \times n$ matrix.

Many results for subsets of a set has an analogue for subspaces of a linear space. The subspace relation is analogous to the subset relation, and defines a partial order. In both partial orders, any two elements have a greatest lower bound (intersection) and a smallest upper bound (union for sets, span for two subspaces). The orthocomplement is analogous to the complement. There will be many examples for this paradigm, which was put in focus by Gian-Carlo Rota.

3 Problems

Finding combinatorial proof is a plus!

Q1) Prove

$$\sum_{k=0}^{h} \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} m \\ h-k \end{bmatrix}_q q^{(n-k)(h-k)} = \begin{bmatrix} m+n \\ h \end{bmatrix}_q .$$

Q2) Prove

$$\begin{bmatrix} n+m+1 \\ m+1 \end{bmatrix}_q = \sum_{j=0}^{n} q^j \begin{bmatrix} m+j \\ m \end{bmatrix}_q .$$

Q3) Prove

$$\sum_{i=0}^{n} (-1)^i \begin{bmatrix} n \\ i \end{bmatrix}_q = \begin{cases} 0, & \text{if } n \text{ odd} \\ (1-q)(1-q^3)(1-q^5)\cdots(1-q^{n-1}), & \text{if } n \text{ even.} \end{cases}$$

Q4) Show that the following polynomial identity in x, q is equivalent to the q-binomial theorem:

$$(x-1)(x-q)\cdots(x-q^{n-1}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{n-k}{2}} (-1)^{n-k} x^k. \tag{3.14}$$

Q5) a) Let us be given a linear space V of dimension n, and a linear space W with x elements over $GF(q)$. Show that $|Hom(V, W)|$, the number of linear maps from V to W, is on the one hand x^n, on the other hand $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x-1)(x-q)\cdots(x-q^{k-1})$.

b) Show the following polynomial identity in variables x, q

$$x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x-1)(x-q)\cdots(x-q^{k-1}). \tag{3.15}$$

c) Observe that for any fixed value of q, the identities (3.14) and (3.15) provide an inverse pair. Hence, for a pair of sequences of complex numbers a_n and b_n,

$$\forall n \;\; a_n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q b_k \quad \text{iff} \quad \forall n \;\; b_n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{n-k}{2}} (-1)^{n-k} a_k.$$

d) Assume that $a_n(q)$ and $b_n(q)$ are polynomials of the variable q with complex coefficients. Then

$$\forall n \;\; a_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q b_k(q) \quad \text{is a polynomial identity}$$

if and only if

$$\forall n \;\; b_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q q^{\binom{n-k}{2}} (-1)^{n-k} a_k(q) \quad \text{is a polynomial identity.}$$

Q6) Show that $q^{\binom{k}{2}}\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the ordinary generating function of the number of partitions into k distinct terms, where every term is between 0 and $n-1$. (We do not specify which number is to be partitioned!) In other words, if $q^{\binom{k}{2}}\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_\ell c_\ell q^\ell$, then $c_\ell =$ the number of partitions of ℓ into k distinct terms, where every term is between 0 and $n-1$.
Q7) Fixing a and a $|q| < 1$, show that the function $F(t) = \prod_{n=0}^{\infty} \frac{1-atq^n}{1-tq^n}$ satisfies the functional equation $(1-t)F(t) = (1-at)F(qt)$, and derive from here the infinite version of the q-binomial theorem.
Q8) Derive Theorem 4 from Theorem 5.
Q9) (a) Substitute $a = q^m$ for some $m \in \mathbb{N}$ into (1.11). What do you obtain?
(b) What is the limit of your identity as $q \to 1$?
(c) Show that $\begin{bmatrix} m+n-1 \\ n \end{bmatrix}_q$ is the ordinary generating function of the number of partitions (of unspecified numbers) into n terms, all terms between 0 and $m-1$. In other words, if $\begin{bmatrix} m+n-1 \\ n \end{bmatrix}_q = \sum_\ell c_\ell q^\ell$, then $c_\ell =$ the number of partitions of ℓ into n terms, all terms between 0 and $m-1$.
(d) Show that $\begin{bmatrix} m+n-1 \\ n \end{bmatrix}_q$ is the ordinary generating function of the number of partitions (of unspecified numbers) into at most $m-1$ terms, all terms between 1 and n. In other words, if $\begin{bmatrix} m+n-1 \\ n \end{bmatrix}_q = \sum_\ell c_\ell q^\ell$, then $c_\ell =$ the number of partitions of ℓ into at most $m-1$ terms, all terms between 1 and n.
Q10) Prove Jacobi's Triple Product Identity: for any $0 \neq z \in \mathbb{C}$ and $q \in \mathbb{C}$ with $|q| < 1$, the following identity holds

$$\prod_{n=1}^{\infty}\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right) = \sum_{n=-\infty}^{\infty} q^{n^2} z^n.$$