Spreading the q-disease: The q-binomial coefficients and their combinatorial interpretation.

Juan Pablo Vigneaux
IMJ-PRG / Université Paris Diderot

December 12, 2017

"By that time, all three of us had already been severely afflicted with the 'q-disease', a dangerous mathematical illness whose earliest victim was Euler, but which was first diagnosed by Richard Askey. Mathematicians working in practically every field, be it algebra, geometry, analysis, differential equations —you name it— are vulnerable to its seductive charm. The first symptom of the q-disease is that one day you realize that most of the results obtained or acquired during your mathematical life admit a q-deformation. The second stage is indicated by the idea that the q-case is much more interesting."

- Etingof, Frenkel, Kirillov

1. The q-derivative

Consider the expression

$$\frac{f(x) - f(x_0)}{x - x_0}. \tag{1}$$

In analysis, we define the (infinitesimal) derivative as the limit of (1) when $x \to x_0$. However, if we just replace x by qx or $x + h$, withour taking the limit, we enter the world of "quantum" calculus (q-calculus or h-calculus). The case of h-calculus correspond to difference equations and won't be treated in this article. We will focus on q-calculus, that has rich relations with number theory and the representation theory of quantum groups. [1]

For any $q \neq 1$, the q-derivative of a function $f : \mathbb{R} \to \mathbb{R}$ is defined as

$$D_q f(x) = \frac{f(qx) - f(x)}{(q-1)x} \equiv \frac{d_q f(x)}{d_q x}. \tag{2}$$

Remark that D_q is a linear operator. We work here on the real numbers, but we could use other field (of characteristic 0, for some constructions bellow); for instance, in representation theory, q is sometimes a complex root of unity.

[1] In this section and the next one, we follow closely the book by Kac [3].

Since $D_q x^n = \frac{q^n-1}{q-1} x^{n-1}$, we define the q-analog of the integer n (a q-integer) by

$$[n] := \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}. \tag{3}$$

With this notation, $D_q x^n = [n] x^{n-1}$.

The q-derivative satisfies a deformed product rule:

$$D_q(f(x)g(x)) = f(qx)(D_q g(x)) + (D_q f(x))g(x); \tag{4}$$

the reader can verify this by direct computation. The commutativity of the product of functions gives a second product rule

$$D_q(f(x)g(x)) = g(qx)(D_q f(x)) + (D_q g(x))f(x). \tag{5}$$

The application of this rule to the equality $g(x)\left(\frac{f(x)}{g(x)}\right) = f(x)$ allows us to deduce a formula for the derivative of a quotient of functions. However, there is no chain rule in q-calculus.

2. Taylor formula

The following proposition generalizes the usual Taylor formula.

Proposition 1. *Let a be a real number; D, a linear operator on $\mathbb{R}[x]$ (polynomials with real coefficients), and $\{P_0(x), P_1(x), P_2(x), ...\}$, a sequence of polynomials satisfying:*

(i) $P_0(a) = 1, \quad P_n(a) = 0$ *for all* $n \geq 1$.
(ii) $\deg P_n = n$.
(iii) $DP_n = P_{n-1}$ *for all* $n \geq 1$ *and* $D(1) = 0$.

Then, for any polynomial $f(x)$ of degree N one has

$$f(x) = \sum_{k=1}^{N} (D^k f)(a) P_k(x). \tag{6}$$

The proof of this proposition is relatively simple. By condition (ii), the set $\{P_i\}_i$ is a base of $\mathbb{R}[x]$. Therefore, f can be expressed as a combination $\sum_{i=0}^{N} c_k P_k$, where c_k are appropriate constants. To find c_0, just evaluate f at a to obtain $c_0 = f(a)$, by condition (i). In virtue of (iii), $f'(x) = \sum_{k=1}^{N} c_k P_{k-1}$, which implies that $c_1 = f'(a)$. By recursion, $c_k = (D^k f)(a)$.

Remark that the same reasoning allows us to express any formal series f as an the infinite linear combination $\sum_{k=0}^{\infty}(D^k f)(a)P_k(x)$; this turns out to be important in the applications to number theory.

The usual Taylor polynomials correspond to the case $D = \frac{d}{dx}$ and $P_n(x) = \frac{(x-a)^n}{n!}$. Of course, we want to set now $D = D_q$... what is the good choice of P_ns? If $a = 0$, we can simply take $P_n(x) = \frac{x^n}{[n]!}$, where $[n]! = [n][n-1]\cdots[1]$. But, in general, $\frac{(x-a)^n}{[n]!}$ does not give the good solution. It is clear that $P_0(x) = 1$ and $P_1(x) = x - a$; in turn, by conditions (iii) and (i), this implies that

$$P_2(x) = \frac{x^2}{[2]!} - ax - \frac{a^2}{[2]!} + a^2 = \frac{(x-a)(x-qa)}{[2]!}. \tag{7}$$

It turns out that, for $n \geq 1$, the good choice is

$$P_n(x) := \frac{(x-a)(x-qa)\cdots(x-q^{n-1}a)}{[n]!}. \tag{8}$$

Following [**?**], we will simply write $(x-a)_q^n$ instead of $(x-a)(x-qa)\cdots(x-q^{n-1}a)$; by convention, $(x-a)_q^0 = 1$. In the theory of hypergeometric functions, the quantity $(1-a)(1-qa)\cdots(1-q^{n-1}a)$ is denoted $(a;q)_n$ and called "the q-Pochhammer symbol".

Proposition 2. *For $n \geq 1$, $D_q(x-a)_q^n = [n](x-a)_q^{n-1}$.*

This is proved by induction on n. For $(x-a)_q^{n+1} = (x-a)_q^n(x-q^na)$, the product rule gives

$$\begin{aligned}
D_q(x-a)_q^{n+1} &= (qx - q^na)D_q(x-a)_q^n + (x-a)_q^n D_q(x-q^na) && (9)\\
&= q(x-q^{n-1}a)[n](x-a)_q^{n-1} + (x-a)_q^n && (10)\\
&= (q[n]+1)(x-a)_q^n = (q(1+\cdots+q^{n-1})+1)(x-a)_q^n && (11)\\
&= [n+1](x-a)_q^n. && (12)
\end{aligned}$$

Therefore, we conclude that:

Proposition 3. *For any polynomial $f(x)$ of degree N and any number $c \in \mathbb{R}$, the following q-Taylor formula is satisfied:*

$$f(x) = \sum_{i=0}^{N}(D_q^j f)(c)\frac{(x-c)_q^j}{[j]!}. \tag{13}$$

Let us apply the formula to $f(x) = (x+a)_q^n$ and $c = 0$. We simply replace

$$D_q^j f(0) = [n]\cdots[n-j+1](0+a)_q^n = [n]\cdots[n-j+1]q^{(n-j)(n-j-1)/2}a^{n-j}, \quad (14)$$

in (13) and then make the change of variables $k = n - j$ to get the so called **Gauss binomial formula**:

$$(x+a)_q^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^{k(k-1)/2} a^k x^{n-k}. \quad (15)$$

The coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ equals $\frac{[n]!}{[k]![n-k]!}$ and —naturally— it is called q-binomial coefficient (or Gaussian binomial coefficient).

There is another binomial theorem that involves the coefficients $\begin{bmatrix} n \\ k \end{bmatrix}$.

Proposition 4. *Suppose that x, y are two variables such that*

$$yx = qxy. \quad (16)$$

Then,

$$(x+y)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k y^{n-k}. \quad (17)$$

Side note: the real algebra generated by x and y under the relation (16) is called "the quantum plane". (Why algebras are planes? Look for "affine algebraic variety"; this is a non-commutative version.)

Proposition 4 can be proved by recursion, using the relation

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}. \quad (18)$$

In turn, this relation can be easily deduced from the definition of $\begin{bmatrix} n \\ k \end{bmatrix}$; it is also a consequence of the second combinatorial interpretation of the q-binomial coefficients described bellow.

3. The q-binomial coefficients

Let us begin by an interpretation of Proposition 4. Recall that the usual binomial coefficients $\binom{n}{k}$ count the number of sequences in $\{x, y\}^n$ such that x appears k times; we call these "n-sequences of type k". Let us imagine each x as a horizontal unitary vector in the plane, pointing to the right; each y as a vertical unitary vector, pointing up; and the concatenation of symbols (from left to right) as concatenation of the corresponding arrows. Then an n-sequence of type k can be interpreted as a path from $(0,0)$ to $(k, n-k)$. For example, the sequence $xyxx$ is

$$\begin{array}{ccccccc} & & (1,1) & \xrightarrow{x} & (2,1) & \xrightarrow{x} & (3,1) \\ & & {\scriptstyle y}\uparrow & & & & \\ (0,0) & \xrightarrow{x} & (1,0) & & & & \end{array}$$

Moreover, two different sequences always give two different paths. The paths from $(0,0)$ to $(k, n-k)$ that just move rightward and upward, and the n-sequences of type k are in bijection; any of these sets has cardinality $\binom{n}{k}$.

The q-binomial works similarly, but now you have to keep track of any permutations between x and y. Given an n-sequence of type k, say s, let $A(s)$ denote the area between the line $x = k$, the line $y = 0$ and the path represented by the sequence s. For example, $A(x^k y^{n-k}) = 0$. Any other path can be transformed into this path, but any time you turn

$$\begin{array}{ccc} \bullet & \xrightarrow{x} & \bullet \\ {\scriptstyle y}\uparrow & & \\ \bullet & & \end{array} \quad \text{into} \quad \begin{array}{ccc} & & \bullet \\ & & {\scriptstyle y}\uparrow \\ \bullet & \xrightarrow{x} & \bullet \end{array} \tag{19}$$

you have to multiply by q; this means that q keeps track of a unit of area that you lost when you turned yx into xy. In general, any n-sequence s of type k can be transformed into $x^k y^{n-k}$ through the iterated application of the transformation (19); at the end, you find $s = q^{A(s)} x^k y^{n-k}$.

The discussion above implies that $\begin{bmatrix} n \\ k \end{bmatrix}$ **is a polynomial in q, and the coefficient of the power q^A counts the number of n-sequences of type k that determine an area A.**

There is another combinatorial interpretation for the q-binomial coefficients; as far as we know, this interpretation is completely unrelated to the previous one. Recall that, for any prime power q, it is possible to define a field with q elements known as the Galois field of order q, $\mathbb{F}_q$.

Proposition 5. *Let q be a prime power. The coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ counts the number of k dimensional vector subspaces of $\mathbb{F}_q^n$.*

Proof. Note that $\mathbb{F}_q^n$ has q^n points. If $k = 0$, then $\begin{bmatrix} n \\ 0 \end{bmatrix} = 1$ counts the only space of dimension 0. When $k \geq 1$, to build a k-dimensional subspace, pick first a vector $v_1 \neq 0$ ($q^n - 1$ possibilities), then a vector v_2 independent of v_1 ($q^n - q$ possibilities, that correspond to the vectors outside $\langle v \rangle$), and continue this way up to v_k ($q^n - q^{k-1}$

possibilities). This means that there are

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}) \tag{20}$$

ways of choosing k independent vectors. But different collection of vectors can give the same subspace (we are double-counting). To count the number of subspaces, we must divide (20) by the number of bases of a k-dimensional subspace. This cardinality is obtained by the same reasoning (pick a first element of the base, then a second independent of the first one...). Therefore,

$$(\text{number of } k \text{ dimensional subspaces} = \frac{(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1})}{(q^k - 1)(q^k - 1)\cdots(q^k - q^{k-1})} = \begin{bmatrix} n \\ k \end{bmatrix}. \tag{21}$$

□

As promised, the Pascal relation

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}. \tag{22}$$

can be deduced from the following observation: let $\{e_1, ..., e_n\}$ be a base of $\mathbb{F}_q^n$ and identify $\mathbb{F}_q^{n-1}$ with $\langle e_1, ..., e_{n-1} \rangle$; a k dimensional subspace is either

- $W \oplus \langle e_n \rangle$, with W a $k-1$ dimensional subspace of $\mathbb{F}_q^{n-1}$;
- The graph of a k dimensional space W' contained in $\mathbb{F}_q^{n-1}$; there are q^k different linear applications that can be defined on W' (the cardinality of the dual of $\mathbb{F}_q^k$).

Some final remarks: Proposition 5 show a very strong analogy between the counting of subsets of a set of cardinality n and the counting of subspaces of $\mathbb{F}_q^n$. One could wonder in which sense an n-element set is like $\mathbb{F}_1^n$. Of course, there is no field of characteristic one, but there are very good reasons to give mathematical content to this analogy. One of these reason is that $\mathbb{Z}$ is expected to be a $\mathbb{F}_1$-algebra, and therefore $\mathrm{Spec}(\mathbb{Z})$ could be thought as a "curve" over $\mathbb{F}_1$. Many people hope that we will be able to reproduce the proof of the Weil conjecture (developed mainly by Grothendieck and Deligne) to prove the Riemann hypothesis. Connes and Consani [2] have defined the "arithmetic site" to move in this direction.

There is a context in which the analogy between sets and spaces can be made precise. Proposition 5 can be modified to prove that $\left[\begin{smallmatrix} n+1 \\ k+1 \end{smallmatrix}\right]$ count the number of k dimensional subspaces of $\mathbb{P}^n(F_q)$, the projective space. Birkhoff defined axiomatically a "projective geometry of order q", where one can find the known projective spaces $\mathbb{P}^n(F_q)$ as particular examples of order q. The Boolean algebra of a finite set is a projective geometry of order 1. Just from the axioms, one can prove the analogous of Proposition 5, and the counting of subsets of a set sits simply as a particular case. See [1].

References

[1] H. Cohn. Projective geometry over f_1 and the gaussian binomial coefficients. *The American Mathematical Monthly*, 111(6):487–495, 2004.

[2] A. Connes and C. Consani. Geometry of the arithmetic site. *Advances in Mathematics*, 291:274–329, 2016.

[3] V. Kac and P. Cheung. *Quantum Calculus*. Universitext. Springer New York, 2001.