MIT 18.211: COMBINATORIAL ANALYSIS

FELIX GOTTI

Lecture 5: Permutation Inversions and q-Binomials

In this lecture, we introduce q-analogs of $n!$ and $\binom{n}{k}$, which are corresponding combinatorial expressions depending on a variable q that when we evaluate at $q = 1$ we recover $n!$ and $\binom{n}{k}$, respectively. Most importantly, in the same way $n!$ and $\binom{n}{k}$ count linear arrangements and k-subsets of a given set of size n, their corresponding q-analogs count chain of subspaces and k-dimensional subspaces of a given vector space of dimension n (over a field of q elements).

Counting Inversions. Let S_n denote the set consisting of all permutations of $[n]$. The *inversion table* of a permutation $w \in S_n$ is an n-tuple $I(w) := (a_1, \dots, a_n)$, where a_i denotes the number of elements j in w to the left of i with $j > i$. Observe that $0 \le a_i \le n - i$ for every $i \in [n]$.

Proposition 1. *For each $n \in \mathbb{N}$, the map $I \colon S_n \to [\![0, n-1]\!] \times [\![0, n-2]\!] \times \cdots \times [\![0, 0]\!]$, where $I(w)$ is the inversion table of w, is a bijection.*

Proof. Set $T_n := [\![0, n-1]\!] \times [\![0, n-2]\!] \times \cdots \times [\![0, 0]\!]$. Since $|S_n| = |T_n| = n!$, it suffices to show that the function I is surjective. Take $(a_1, \dots, a_n) \in T_n$ and let us construct $w \in S_n$ as follows. Consider the element n as an initial linear arrangement of length 1. Then suppose that we have inserted the elements $n-1, n-2, \dots, n-i+1$ (in this order) into the initial length-1 linear arrangement. In the i-th step, insert $n - i$ in the current length-i linear arrangement so that there are exactly a_{n-i} elements to the left of $n - i$. After inserting 1, we obtain a length-n linear arrangement of $[n]$, that is, a permutation $w \in S_n$. Observe that in our construction of w, right after we inserted $n - i$ there were precisely a_{n-i} elements j in the linear arrangement to the left of $n - i$ such that $j > n - i$, and this number was unchanged during the remaining steps as only elements less than $n - i$ were inserted then. Hence $I(w) = (a_1, \dots, a_n)$, and we can conclude that I is a surjective. $\square$

An *inversion* of $w := w_1 w_2 \cdots w_n \in S_n$ is a pair (w_i, w_j) such that $i < j$ but $w_i > w_j$. The number of inversions of a permutation w is denoted by $\mathrm{inv}(w)$. Observe that if $I(w) = (a_1, \dots, a_n)$ is the inversion table of w, then $\mathrm{inv}(w) = a_1 + \cdots + a_n$.

Proposition 2. *The identity*

$$\sum_{w \in S_n} q^{\mathrm{inv}(w)} = (1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{n-1})$$

holds for every $n \in \mathbb{N}$.

Proof. Set $T_n := [0, n-1] \times [0, n-2] \times \cdots \times [0, 0]$. Since the assignment $w \mapsto I(w)$ induces a bijection $S_n \to T_n$, and $\mathrm{inv}(w) = a_1 + \cdots + a_n$ for every $w \in S_n$ with $I(w) = (a_1, \dots, a_n)$, it follows that

$$\begin{aligned}\sum_{w \in S_n} q^{\mathrm{inv}(w)} &= \sum_{(a_1,\dots,a_n) \in T_n} q^{a_1+\cdots+a_n} = \sum_{a_1=0}^{n-1}\sum_{a_2=0}^{n-2}\cdots\sum_{a_n=0}^{0} q^{a_1}q^{a_2}\cdots q^{a_n} \\ &= \sum_{a_1=0}^{n-1} q^{a_1} \sum_{a_2=0}^{n-2} q^{a_2} \cdots \sum_{a_n=0}^{0} q^{a_n} = \prod_{k=0}^{n-1}(1+q+\cdots+q^k),\end{aligned}$$

which yields the desired identity. □

Motivated by the previous proposition, for every $n \in \mathbb{N}$ we define the following q-analogs

$$(n)_q := 1 + q + \cdots + q^{n-1} \quad \text{and} \quad (n)_q! := (1)_q(2)_q\cdots(n)_q,$$

of n and $n!$, respectively. By convention, we set $(0)_q = 0$, and so $(0)_q! = 1$. We call $(n)_q!$ the *q-factorial* of n. In general, and roughly speaking, a q-analog of a mathematical object, is another mathematical object depending on a variable q that specializes to the former object when $q = 1$. One can see that $(n)_1 = n$ and $(n)_1! = n!$. Observe that we can also write $(n)_q$ and $(n)_q!$ as follows:

$$(n)_q = \sum_{j=0}^{n-1} q^j = \frac{q^n - 1}{q-1} \quad \text{and} \quad (n)_q! = \prod_{k=1}^{n} \frac{q^k-1}{q-1}.$$

Counting Subspaces. Using the previous q-analog of $n!$, we can naturally define q-analogs for the binomial coefficients:

$$\binom{n}{k}_q := \frac{(n)_q!}{(k)_q!(n-k)_q!}$$

for every $n \in \mathbb{N}_0$ and $k \in [\![0, n]\!]$. It is clear that $\binom{n}{k}_q$ is a q-analog of $\binom{n}{k}$, and the former is called a *q-binomial coefficient*. As the next proposition indicates, $\binom{n}{k}_q$ counts the set of k-dimensional subspaces of an n-dimensional vector space over a finite field of size q[1]. Let $\mathbb{F}_q$ denote a finite field such that $|\mathbb{F}_q| = q$. As for vector spaces over $\mathbb{R}$, a vector space over $\mathbb{F}_q$ of dimension d can be treated as (i.e., is isomorphic to) $\mathbb{F}_q^d$.

[1]There exists a finite field of size q precisely when q is a positive power of a prime, in which case there is exactly one field of size q (up to isomorphism).

Proposition 3. *For all $n \in \mathbb{N}_0$ and $k \in [\![0, n]\!]$, the number of k-dimensional subspaces of the vector space $\mathbb{F}_q^n$ is $\binom{n}{k}_q$.*

Proof. Let $A(n, k)$ denote the number of k-dimensional subspaces of $\mathbb{F}_q^n$, and let $L(n, k)$ denote the number of sequences consisting of k linearly independent vectors in $\mathbb{F}_q^n$. We proceed to count the number $L(n, k)$ of k-sequences $v_1, \dots, v_k$ of linearly independent vectors in $\mathbb{F}_q^n$ in two different ways. Choose v_1 to be any nonzero vector of $\mathbb{F}_q^n$, which can be done in $q^n - 1$ different ways. Then choose v_2 in $\mathbb{F}_q^n$ so that v_2 is not a multiple (i.e, a linear combination) of v_1; this can be done in $q^n - q$ ways. In the i-th step, choose v_i in $\mathbb{F}_q^n$ so that it is not a linear combination of $v_1, \dots, v_{i-1}$, which can be done in $q^n - q^{i-1}$ different ways. Therefore

$$L(n, k) = (q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}). \tag{0.1}$$

We can also obtain $L(n, k)$ as follows. First, we choose a k-dimensional subspace W of $\mathbb{F}_q^n$ in $A(n, k)$ possible ways, and then we choose a linearly independent sequence of k vectors in $W \cong \mathbb{F}_q^k$, which can be done in $(q^k - 1)(q^n - q) \cdots (q^k - q^{k-1})$ by mimicking the way we just described above to choose a sequence of k linearly independent vectors of $\mathbb{F}_q^n$. As a result, $L(n, k) = A(n, k)(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})$, and taking into account the equality (0.1) we obtain

$$\begin{aligned} A(n, k) &= \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} \\ &= \frac{\prod_{j=1}^{n} \frac{q^j - 1}{q - 1}}{\prod_{j=1}^{k} \frac{q^j - 1}{q - 1} \prod_{j=1}^{n-k} \frac{q^j - 1}{q - 1}} \\ &= \frac{(n)_q!}{(k)_q! \cdot (n-k)_q!} = \binom{n}{k}_q . \end{aligned}$$

∎

Practice Exercises

Exercise 1. *For $n \in \mathbb{N}$, argue that there are $(n)_q!$ ordered sequences $V_1, \dots, V_n$ of subspaces of $\mathbb{F}_q^n$ with $\dim V_i = i$ for every $i \in [n]$ such that $V_1 \subset V_2 \subset \cdots \subset V_n$.*

Exercise 2. *For any $n \in \mathbb{N}_0$ and $k \in [\![0, n]\!]$, prove that*

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k} \binom{n-1}{k-1}_q .$$

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu