Lecture 14

Lecture date: March 31, 2011 *Notes by: Leon Zhou*

1 q-binomial coefficients

1.1 Connection to partitions

Let $a_l = \#\{\text{partitions } \lambda \text{ of } l \big| \text{the Young diagram of } \lambda \text{ fits in a box of dimensions } k \times (n-k)\}$.

Theorem 1

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{l=0}^{k(n-k)} a_l q^l$$

Proof: Fix a flag $E_0 \subset E_1 \subset \ldots \subset E_n$ of $\mathbb{F}_q^n$. Given a k-subspace V, let $d_i = \dim(V \cap E_i)$, and write $\underline{d} = (d_0, d_1, \ldots d_n)$.

Now, given $\underline{d}$, let $f(\underline{d}) = \#(k\text{-subspaces } V \subset \mathbb{F}_q^n | \dim V \cap E_i = d_i, i \in \{0, \ldots n\})$.

Lemma 2 *$f(\underline{d}) = q^{m_1 - 1} q^{m_2 - 2} \ldots q^{m_k - k}$, where $m_i = \min\{j | d_j = i\}$*

Recall from last time: $\#\{\text{lines } \{0\} \in L \subset V | L \not\subset H\} = [n]_q - [n-1]_q = q^{n-1}$, where H is a hyperplane in $\mathbb{F}_q^n$.

We want to count the number of ways to choose a k-subspace V.

Define $V_i = V \cap E_{m_i}$, where $\dim V_i = i$. Choosing V is the same as choosing the sequence $(V_i)_{0 \le i \le k}$, since the intersections of V with our flag define V.

To choose $V_1 = V \cap E_{m_1}$ is to choose a line in E_{m_1} that is not contained in $E_{m_1 - 1}$. As we recalled, there are $q^{m_1 - 1}$ ways to do this.

To choose $V_2 = V \cap E_{m_2}$ is to choose a line in E_{m_2}/V_1 that is not contained in $E_{m_2 - 1}/V_1$. There are $q^{m_2 - 2}$ ways to do this.

In general, to choose $V_j = V \cap E_{m_j}/V_{j-1}$ is to choose a line in E_{m_j}/V_{j-1} that is not contained in $E_{m_j - 1}/V_{j-1}$, and there are $q^{m_j - j}$ ways to do this.

—

So $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k-subspaces of $\mathbb{F}_q^n$. But this is equal to

$$\sum_{\underline{d}} f(\underline{d})$$

where the sum ranges over all sequences $\underline{d} = (d_0, \ldots d_n)$ with $0 = d_0 \leq \cdots \leq d_n = k$ and $d_{i+1} - d_i \leq 1$ for all i.

Given a sequence $\underline{d}$, we form a southwest lattice path, where step i is

- S, if $d_{i+1} = d_i$, and
- W, if $d_{i+1} = d_i + 1$.

starting at $(k, 0)$ and ending at $(0, k - n)$.

This draws a Young diagram for a partition we can call λ; then $|\lambda|$ is the number of boxes above the lattice path, which is equal to

$$c_1 + c_2 + \ldots + c_k$$

where c_j is the height of column j.

Note that $c_i = m_i - i$, since all but c_i of the steps before column i are westward.

So

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\underline{d}} f(\underline{d}) = \sum_{\lambda \text{ in box}} q^{|\lambda|} = \sum_{l=0}^{k(n-k)} a_l q^l$$

1.2 The q-Binomial Theorem

So there's this Binomial Theorem $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ and we might ask whether we can come up with an analagous formula in q-binomial coefficients.

As it turns out, we can. Consider the algebra $A = \mathbb{Q}[q] < x, y > /(yx - qxy)$, the polynomials in three variables q, x, y over $\mathbb{Q}$ in which q commutes with everything but $yx = qxy$. Say we try to do some binomial expansion:

$$\begin{aligned}(x+y)^3 &= (x+y)(x+y)(x+y)\\ &= xxx + xxy + xyx + yxx + xyy + yxy + yyx + yyy\\ &= xxx + xxy + qxxy + qx(qxy) + xyy + qxyy + q(qxy)y + yyy\\ &= x^3 + x^2y + qx^2y + q^2x^2y + xy^2 + qxy^2 + q^2xy^2 + y^3\\ &= x^3 + (1+q+q^2)x^2y + (1+q+q^2)xy^2 + y^3\\ &= \sum_{k=0}^{3} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k y^{n-k}\end{aligned}$$

As it turns out, this is true in general (see homework #5).

1.3 Counting irreducible monic polynomials

Question 3 *How many irreducible monic polynomials $f(x) = a_0 + a_1x + \ldots + a_nx^n$ of degree n are there in $\mathbb{F}_q[x]$?*

Say we make a list $f_1(x), f_2(x)\ldots$ of all the monic irreducible polynomials in $\mathbb{F}_q[x]$, and let $d_i = \deg(f_i(x))$. By unique factorization, any monic polynomial $f(x) \in \mathbb{F}_q[x]$ can be written uniquely as a product $\prod_{i\geq 1} f_i(x)^{a_i}$ (where all but finitely many a_i are 0).

This leads to a bijection between the set of monic polynomials of degree n and the set of sequences

$$(a_1, a_2, \ldots) \text{ such that } a_1d_1 + a_2d_2 + \ldots = n$$

In other words, partitions of n into piles of size d_i.

We can write a generating function for these partitions:

$$\frac{1}{(1-x^{d_1})(1-x^{d_2})\ldots}$$

Then, since the number of monic polynomials in $\mathbb{F}_q[x]$ of degree n in just q^n, our bijection tells us that we have

$$\frac{1}{(1-x^{d_1})(1-x^{d_2})\ldots} = \sum_{n=0}^{\infty} q^n x^n = \frac{1}{1-qx}$$

Taking the log of both sides:

$$\log \frac{1}{1-x^{d_1}} + \log \frac{1}{1-x^{d_2}} + \ldots = \log \frac{1}{1-qx}$$
$$= \sum_{n \geq 1} \frac{(qx)^n}{n}$$

We can rewrite the left hand side as

$$\sum_{d=1}^{\infty} N_d \log \frac{1}{1-x^d}$$

where N_d is the number of irreducible monic polynomials of degree d over $\mathbb{F}_q$, since there are N_d terms in the left hand sum for which $d_i = d$. And

$$\sum_{d=1}^{\infty} N_d \log \frac{1}{1-x^d} = \sum_{d=1}^{\infty} N_d \sum_{j \geq 1} \frac{x^{dj}}{j} = \sum_{n \geq 1} \sum_{d|n} \frac{N_d}{n/d} x^n$$

where the second equality is obtained by substituting n for dj.

Equating coefficients:

$$\sum_{n \geq 1} \sum_{d|n} \frac{N_d}{n/d} x^n = \sum_{n \geq 1} \frac{(qx)^n}{n}$$
$$\implies \frac{q^n}{n} = \frac{1}{n} \sum_{d|n} dN_d$$
$$q^n = \sum_{d|n} dN_d$$
$$\overset{\text{Möbius Inversion}}{\implies} nN_n = \sum_{d|n} q^d \mu(\frac{n}{d})$$
$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Hey, this expression on the right is equal to the number of rotation classes of primitive necklaces of length n, using q colors of beads!

Example 4 *If p is a prime, then $N_p = \frac{1}{p}(q^p - q)$.*

2 Hyperplane Arrangements

2.1 Definitions

Definition 5 *Given a vector space V with $\dim V = l$, a hyperplane arrangement is a finite set of hyperplanes*

$$A = \{H_1, \ldots, H_n | H_i \text{ is an } (l-1)\text{-dimentional subspace of } V\}$$

A is defined over $\mathbb{Z}$ if $H_i = \{x \in V | \sum c_{ij} x_i = b_i; b_i, c_{ij} \in \mathbb{Z}\}$– that is, if the equations defining the H_i have integer coefficients.

Note that we implicitly take a basis for V in this definition.

Definition 6 *The intersection poset of A is the set of subspaces*

$$L(A) = \left\{ \bigcap_{i \in I} H_i \mid I \subseteq [n] \right\}$$

ordered by inclusion.

Note that $\emptyset$ is not actually a subspace of V, so $L(A)$ may not have a minimal element. It does have a maximal element, V.

Definition 7 *A is central if every H_i passes through the origin; i.e., if $b_i = 0$ in every defining equation.*

On the other hand, if A is central, then it does have a minimal element, $\bigcap_{i=1}^n H_i$, which contains 0 and is thus nonempty. In this case $L(A)$ is actually a lattice, where $H_i \wedge H_j = H_i \cap H_j$.

2.2 Connection to finite fields

Given a hyperplane arrangement which is defined over $\mathbb{Z}$, we can take the defining equations $\sum c_{ij} x_i = b_i \pmod q$ to get a hyperplane arrangement over $\mathbb{F}_q$.

Question 8 *How many points of $\mathbb{F}_q^l$ are in the complement of the arrangement? i.e., what is $\#\left(\mathbb{F}_q^l - \bigcup_{i=1}^n H_i\right)$?*

We can use the Principle of Inclusion-Exclusion:

$$q^l - \sum_{i=1}^{n} q^{l-1} + \sum_{i,j,H_i \cap H_j \neq 0} q^{l-2} - \dots$$

That doesn't seem to be very productive. In general, when we see complicated subscripts on sums like we have here, that's a sign that we should try something else, like Möbius Inversion.

Let $\chi(A, q) = \#(\mathbb{F}_q^l - \bigcup_{i=1}^n H_i)$ be the size of the complement of A.

Lemma 9

$$\chi(A, q) = \sum_{X \in L(A)} \mu(X, \hat{1}) q^{\dim X}$$

Recall that $\hat{1} = V = \mathbb{F}_q^l$.

Proof: For $Y \in L(A)$, let $f(Y) = \#\{v \in \mathbb{F}_q^l \mid v \in Y \text{ and } v \notin Z \text{ for } Z < Y\}$.

Then $\chi(A, q) = f(\hat{1})$, and

$$\sum_{Z \leq Y} f(Z) = \#Y = q^{\dim Y}$$

Define $g(Y) := q^{\dim Y}$.

Invert:

$$f(Y) = \sum_{Z \leq Y} \mu(Z, Y) q^{\dim Y}$$

Let $Y = \hat{1}$; then we are done. □

The polynomial $\chi(A, q)$ is called the characteristic polynomial of A.

Example 10 *The Braid arrangement is* $B_n := \{H_{ij} | 1 \leq i < j \leq n\}, H_{ij} = \{x_i = x_j\}$ *in* $\mathbb{F}_q^n$.

$$\begin{aligned} \chi(B_n, q) &= \#\{v \in \mathbb{F}_q^n | \text{all the coordinates } v_i, \dots v_n \text{ are distinct}\} \\ &= \binom{q}{n} n! = q(q-1)(q-2)\dots(q-n+1) \end{aligned}$$

□