Lecture 13

Lecture date: Mar 29, 2011 *Notes by: Alex Arkhipov*

1 Introduction

Today, we're going to introduce q-analogues, which are a refinement of binomial coefficients. To understand q-analogues combinatorially, we'll show how they arise from counting problems on the lattice of vector spaces over a finite field.

2 Review of Finite Fields

We expect you already know what a field is: an algebraic structure in which you can add, subtract, multiply, and divide, and has 0 and 1 elements that behave like you'd expect them to. You can look up the field axioms.

A field may have $1 + 1 + \cdots + 1 = 0$ for some number of ones. In fact, for a finite field, this must be the case for some number of ones, and the minimum such number of ones is the field's *characteristic*. There is exactly one finite field with q elements (written $\mathbb{F}_q$) for each q that is a power of a prime, $q = p^m$. This field has characteristic p. When $m = 1$, the field $\mathbb{F}_p$ is the familiar field $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p.

3 The Subspace Lattice and Flags

Let $\mathbb{F}_q^n$ be the vector space of n-tuples of elements of the field $\mathbb{F}_q$. We're going to concentrate on one combinatorial object, the lattice of linear subspaces of $\mathbb{F}_q^n$ ordered by inclusion.

Definition 1 *Define $L_n(q)$ to be the lattice of linear subspaces of $\mathbb{F}_q^n$ partially ordered by inclusion. The meet $V \wedge W$ is given by the intersection $V \cap W$ and the join $V \vee W$ by the sum $V + W = span(V \cup W)$.*

In the definition of $L_n(q)$, we do not take the empty set to be a subspace.

Definition 2 *A **flag** (also called a **complete flag**) is a maximal chain in $L_n(q)$.*

So, a flag is a sequence of subspaces one dimension higher than and containing the previous. For the chain to be maximal, it must contain $n+1$ subspaces, whose dimensions start at 0 and count up through n.

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_n = \mathbb{F}_q^n.$$

Note that $dim(E_i) = i$.

Here's the question we'd like to answer:

Question 3 *How many flags of $\mathbb{F}_q^n$ are there (call this $f_n(q)$)?*

Since one can specify a flag by choosing spaces $E_0, E_1, \ldots, E_n$ in sequence, we will count the number of choices at each step.

E_0: No choice, must be $\{0\}$.

E_1: We're choosing a line through the origin. It suffices to choose any nonzero point $v \in \mathbb{F}_q^n - \{0\}$ and let E_1 be the subspace its spans $\langle v \rangle$, and there are $q^n - 1$ ways to do this. But, since $\langle v \rangle = \langle \lambda v \rangle$ for any nonzero scalar λ of $\mathbb{F}_q$, we're overcounting by a factor of $q-1$. So, there are $\frac{q^n-1}{q-1}$ choices.

E_2: We wish to extend $E_1 = \langle v_1 \rangle$ by adding a new vector so that $E_2 = \langle v_1, v_2 \rangle$. Any $v_2 \in \mathbb{F}_q^n - \langle v_1 \rangle$ works, of which there are $q^n - q$. But since $\langle v_1, v_2 \rangle = \langle v_1, \lambda v_2 + w \rangle$ for any $\lambda \in \mathbb{F}_q - \{0\}$ and $w \in E_1$, there are $\frac{q^n-q}{q(q-1)}$ choices.

E_k: In general, having chosen $E_{k-1} = \langle v_1, v_2, \ldots, v_{k-1} \rangle$, there are $q^n - q^{k-1}$ choices of $v_k \in \mathbb{F}_q^n - E_{k-1}$, and since $\langle v_1, v_2, \cdots, v_{k-1}, v_k \rangle = \langle v_1, v_2, \cdots, v_{k-1}, \lambda v_k + w \rangle$ for $\lambda \in \mathbb{F}_q - \{0\}$ and $w \in E_{k-1}$, there are $\frac{q^n-q^{k-1}}{(q-1)q^{k-1}}$ choices at this step.

Multiplying out the number of choices at each step, we find that

$$f_n(q) = \frac{q^n-1}{q-1} \times \frac{q^n-q}{(q-1)q} \times \cdots \times \frac{q^n-q^{n-1}}{(q-1)q^{n-1}},$$

or simplified,

$$f_n(q) = \frac{q^n-1}{q-1} \times \frac{q^{n-1}-1}{q-1} \times \cdots \times \frac{q-1}{q-1}.$$

We note that the top and bottom contain equally many factors of $q-1$, and cancelling them allows $f_n(q)$ to be expressed as a polynomial.

$$f_n(q) = \left(1+q+\cdots+q^{n-1}\right)\left(1+q+\cdots+q^{n-2}\right)\cdots\left(1+q+q^2\right)(1+q)(1).$$

4 q-Analogues

We'll see in this section how the notions and formulas we've derived for the lattice $L_n(q)$ look like polynomial-in-q versions of the corresponding notions for the Boolean algebra B_n. We call these q-analogues.

We note that plugging in $q = 1$ gives $f_n(1) = n!$. Though there's no field with one element, $n!$ is the number of maximal chains of the Boolean algebra B_n. (There is a not fully-understood notion of B_n acting like a "'field with one element" version of $L_n(q)$) Each maximal chain of B_n is given by a permutation of $[n]$, analogous to a flag being a maximal chain of $\mathbb{F}_q^n$. Looking at the products

$$f_n(q) = \left(1 + q + \cdots + q^{n-1}\right)\left(1 + q + \cdots + q^{n-2}\right)\cdots\left(1 + q + q^2\right)(1 + q)$$

and

$$n! = n \times (n-1) \times \cdots \times 2 \times 1,$$

it makes sense to identify each number k with it's q-analogue $1 + q + \cdots + q^{k-1}$, which we abbreviate as $[k]_q$.

Here's a summary of the q-analogue correspondence.

Concept	q-analogue
n	$[n]_q = 1 + q + \cdots q^{n-1}$
$n!$	$[n]_q! = [1]_q[2]_q \cdots [n]_q$
B_n	$L_n(q)$
S_n	flags in $\mathbb{F}_q^n$
$\binom{n}{k}$	$\begin{bmatrix} n \\ k \end{bmatrix}_q$

5 q-binomial coefficients

The rest of today's lecture will look at the the last row of the table, the q-analogue of $\binom{n}{k}$, which we'll denote as $\begin{bmatrix} n \\ k \end{bmatrix}_q$. If $\binom{n}{k}$ is the number of subsets of n of size k, then $\begin{bmatrix} n \\ k \end{bmatrix}_q$ should be the number of k-dimensional subspaces of $\mathbb{F}_q^n$ (k-subpaces for short). We'll show that $\binom{n}{k}$ is related to $[n]!$ in the same way as $\binom{n}{k}$ to factorials.

Lemma 4

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

Proof: We'll count in two ways the pairs (V, E) where V is a k-subspace of $\mathbb{F}_q^n$ and E is a flag $(E_0, \ldots, E_n)$ of $\mathbb{F}_q^n$ for which $E_k = V$.

For the first way, first choose a flag E; there are $[n]_q!$ choices. Since each E has a unique subspace $V = E_k$, there are $[n]_q!$ pairs.

For the second way, fix V, of which there are $\begin{bmatrix} n \\ k \end{bmatrix}_q$ choices. Now, we're left to choose $(E_0, \ldots, E_{k-1})$ with

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_k = V$$

and $(E_{k+1}, \ldots, E_n)$ with

$$V = E_k \subset E_{k+1} \subset \cdots \subset E_n = \mathbb{F}_q^n.$$

The first choice corresponds to a flag in $\mathbb{F}_q^k$, of which there are $[k]_q!$. For the second, we note that the sublattice of $\mathbb{F}_q^n$ of subspaces containing the k-subspace V is isomorphic to $L_{n-k}(q)$ via modding out by V. So, there are as many choices as flags of $L_{n-k}(q)$, of which there are $[n-k]_q!$. So, the overall number of pairs is

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \times [k]_q! \times [n-k]_q!.$$

So,

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

which gives the result. □

Let's work through an example.

Example 5 *How many 2-subspaces are there of $\mathbb{F}_q^4$?*

Answer 6

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4]_q!}{[2]_q![2]_q!} = \frac{(q^4-1)(q^3-1)(q^2-1)(q-1)}{(q^2-1)(q-1)\times(q^2-1)(q-1)} = (q^2+1)(q^2+q+1) = q^4+q^3+2q^2+q+1$$

Note how the rational functions cancel to produced a polynomial, moreover one whose coefficients are non-negative integers. This should tip you off that these coefficients are counting something. But before we get to that, let's show that this is true in general by means of a recurrence.

Lemma 7

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

(Note that when $q = 1$, we get the usual recurrence for $\binom{n}{k}$.)

Proof: Fix a hyperplane ($(n-1)$-subspace) $H \subset \mathbb{F}_q^n$. We'll split the k-subspaces V that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ counts into two categories.

If $V \subset H$, there are $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ choices of V.

If $V \not\subset H$, then let W be the $(k-1)$-subspace $W = H \cap V$. There are $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ possible W within H. For each W, the k-subspaces V with $W = H \cap V$ are exactly those k-subspaces V with $W \subset V \subset \mathbb{F}_q^n$, excluding those with $W \subset V \subset H$. Modding out by W, these are in one-to-one correspondence with lines (1-subspaces) in $\mathbb{F}_q^n/W$ and H/W respectively, so the number of eligible V is

$$[n-k+1]_q - [n-k]_q = q^{n-k}.$$

So, overall, there are $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q q^{n-k}$ k-subspaces V with $V \not\subset H$. □

From the recurrence, we see that we can build the q-analogue of Pascal's Triangle, where each entry is in row i is the the entry above it plus q^i times the entry to its left.

1	1	1	1	1
1	$q+1$	q^2+q+1	q^3+q^2+q+1	
1	q^2+q+1	$q^4+q^3+2q^2+q+1$		
1	q^3+q^2+q+1			
1				

6 Partitions

Now that we know that the coefficients of the q-binomial $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are non-negative integers, we'd like to understand what they count. We'll see that they count a certain type of partition.

Definition 8 *A* partition *of l is a sequence of natural numbers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l \geq 0$ whose sum is l.*

Partitions are like the compositions we defined before, except reorderings, which is achieved by writing the parts in decreasing order. We may have fewer than l parts by having all remaining parts equal zero. For example, there are five partitions of 4, which are (omitting zero parts) 4, 3+1, 2+2, 2+1+1, and 1+1+1+1.

Definition 9 *The **Young Diagram** of a partition of l is the union of λ_1 boxes in row 1, λ_2 boxes in row 2, and so on. Equivalently, it is the set of pairs (i, j) with $i, j > 0$ and $j \leq \lambda_i$. We say that a partition fits in an $a \times b$ box if all pairs (i, j) have $i \leq a$ and $j \leq b$.*

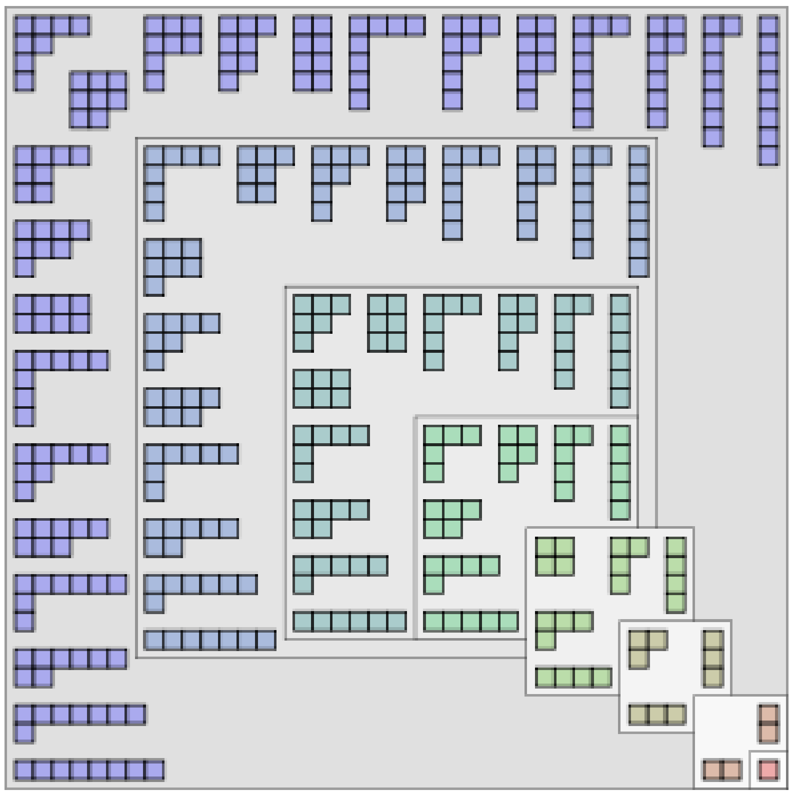

Figure 1: Young Diagrams of all partitions of the numbers 1 through 8. From Wikipedia.

Theorem 10

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

where a_l is number of partitions of l whose Young Diagram fits in a $k \times (n-k)$ box.

For example, corresponding to the polynomial $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1$ is the fact that one partition of four fits in a 2×2 box, as do one partition of 3, two partitions of 2, one partition of 1, and one partition of 0 (the empty partition), which can be counted from in Figure 1.

We'll prove the theorem next class, but today let's note a couple of things.

First, $\begin{bmatrix} n \\ k \end{bmatrix}_q$ has degree $k(n-k)$, which we could have checked from the degrees of the q-factorial terms in its definition.

Second, this theorem makes clear that $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$, since the expression is symmetric with respect to k and $n-k$.

Third, it exposes another symmetry, that the coefficients of each q-binomial are palindromic. This follows from the one-to-one correspondence in which a Young Diagram of a partition of l inside a $k \times (n-k)$ box has its complement taken and is rotated 180 degrees, to produce the Young Diagram of a partition of $k(n-k) - l$ inside a $k \times (n-k)$ box.

Finally, taking $q = 1$, we have the $\binom{n}{k}$ equals the total number of partitions that fit in a $k \times n - k$ box. How can we understand this combinatorially? Observe that the right and bottom boundary of the Young Diagram uniquely defines a path from the bottom left corner to the top right corner of the $k \times (n-k)$ box, made of unit steps going up or right. There are k ups and $n-k$ rights, and their sequence defines a subset of k of n. In this way, we see that q-binomials $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are a more refined count of subset of n of size k, groups by how much area the corresponding path bounds.