Math 4700/6700 – Combinatorics – Spring 2019

Extra Questions for Topic 1

q-Analogs of combinatorial quantities

There are analogs of quantities like $n!$ and $\binom{n}{k}$ that involve a parameter, conventionally denoted q. These are called *q-analogs*. There are also q-analogs of various formulae, particularly binomial coefficient identities.

These q-analogs can be interpreted in various ways. They can be thought of as counting things in vector spaces over the finite field with q elements. In general, there is a field with q elements if and only if q is a prime power, i.e., $q = p^k$ for some prime p and some $k \geq 1$. This field is usually denoted $\mathrm{GF}(q)$, where GF stands for Galois Field, and is unique up to isomorphism.

When $q = p^1$ is actually a prime p, then $\mathrm{GF}(q)$ is just $\mathbb{Z}_p$, the integers modulo p, with the usual addition modulo p and multiplication modulo p. But if q is not a prime, the structure of $\mathrm{GF}(q)$ is more complicated.

I will use $\mathrm{GF}(q)^n$ to denote the n-dimensional vector space over $\mathrm{GF}(q)$, consisting of vectors $(x_1, x_2, \ldots, x_n)$ where $x_i \in \mathrm{GF}(q)$ for each i, with addition and scalar multiplication defined componentwise. In other words, this behaves just like $\mathbb{R}^n$, except that we are using numbers from $\mathrm{GF}(q)$ instead of from $\mathbb{R}$. A key fact is that a k-dimensional vector space (or subspace) over $\mathrm{GF}(q)$ has exactly q^k elements. (That is the number of linear combinations you can form from k basis elements, since there are q choices for each coefficient.)

The q-analogs of things like factorials can also be regarded as generating functions in a variable q, that correspond to generating functions of certain permutation statistics. So they have meaning even when q is not a prime power.

Generally when you substitute $q = 1$, you obtain ordinary combinatorial quantities. So q-factorials become ordinary factorials, and q-binomial coefficients become ordinary binomial coefficients. Thus in some sense working with sets is working with vector spaces over a 1-element field, if that makes any sense!

So now we will actually define these. I will use the following notation.

First, $[n]_q$, for a nonnegative integer n, means

$$[n]_q = 1 + q + q^2 + \ldots + q^{n-1}.$$

If $q \neq 1$, this can also be expressed as $[n]_q = \dfrac{q^n - 1}{q - 1}$. Note that $[0]_q = 0$ and $[1]_q = 1$ for any value of q. And for any nonnegative integer n, $[n]_1 = n$, so that we recover ordinary numbers by putting $q = 1$.

Second, $[n]_q!$, the *q-factorial* of n, just means

$$[n]_q! = [n]_q[n-1]_q[n-2]_q \ldots [2]_q[1]_q.$$

Note that $[0]_q! = 1$ for any value of q.

Third, $\binom{n}{k}_q$, the *q-binomial coefficient* or *Gaussian coefficient*, may be defined as

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}$$

for integers n, k with $0 \leq k \leq n$. If $k < 0$ or $k > n$ we define this to be 0.

Now we provide some problems. The rule for these is as follows. You may substitute up to three X problems (any three) for three regular homework problems. The first X problem must substitute for 1.18, the second for 1.21 and the third for 1.23. So, for example, if you do two X problems you will do X?, X??, 1.23 and 1.25 for the homework on binomial coefficients.

In solving the following problems, you may use results from an earlier problem when proving a later problem. For example, when solving X3 you may use X1 and X2 (even if you did not solve X1 and X2 yourself). In any questions discussing $\mathrm{GF}(q)^n$ or related vector spaces you may assume that q is a prime power.

Note that if we prove a q-analog equation for all prime powers q, then it generally follows (from polynomial interpolation results) that the equation holds for any value of q (real or even complex), as long as bad things like 0 denominators do not happen.

Warning: This problem sheet is in its first iteration and there may be bugs (i.e., mistakes!) in some of the problems.

X1. Prove that the number of ordered bases $(v_1, v_2, v_3, \ldots, v_n)$ of $\mathrm{GF}(q)^n$ is $(q^n - 1)(q^n - q)(q^n - q^2)\ldots(q^n - q^{n-1})$ and express this in terms of $[n]_q!$.

X2. Prove that $[n]_q!$ is the number of sequences of subspaces $\{0\} = V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_{n-1} \subset V_n = \mathrm{GF}(q)^n$, where V_i is an i-dimensional subspace of $\mathrm{GF}(q)^n$. In more technical language, show that $[n]_q!$ is the number of maximal chains in the lattice of vector subspaces of $\mathrm{GF}(q)^n$.

X3. Prove that if no power of q is equal to 1, then $\binom{n}{k}_q = \dfrac{(q^n - 1)(q^{n-1} - 1)\ldots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\ldots(q - 1)}$.

X4. Prove that the number of k-dimensional subspaces of $\mathrm{GF}(q)^n$ is $\binom{n}{k}_q$.

X5. (a) Prove by algebraic manipulation that $\binom{n}{k}_q = \binom{n}{n-k}_q$.

(b) Prove, either by algebraic manipulation (assuming no power of q is equal to 1) or by a combinatorial (counting) argument (in which case you may assume that q is a prime power) that

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

(This is the q-analog of our usual formula $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.)

(c) Use (b) to prove that the Gaussian coefficients $\binom{n}{k}_q$ are not just rational functions of q, they are actually polynomials in q.

X6. Determine the exponents e_i (which may depend on m, n and k as well as i) that make the following identity valid:

$$\binom{n+m}{k}_q = \sum_{i=0}^{k} q^{e_i}\binom{n}{i}_q\binom{m}{k-i}_q.$$

(Of course you must prove that the formula is correct with your values of e_i.)