Joseph C. McGuire
Dr. Anthony Mendes

Homework # 7

MATH 530
October 19, 2024

37.

Prove these identities without writing $\begin{bmatrix} n \\ k \end{bmatrix}_q$ as a fraction and manipulating power of q. Instead, interpret both sides of the identity as rearrangements or integer partitions and show the result by double counting or bijection.

a.

(The $q-$Pascal identity)

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

Proof. Note that from Theorem 1.9(Mendes & Remmel) we have that:

$$\sum_{\text{partitions } \lambda \text{ with Young Diagrams fitting in a } k\times(n-k) \text{ Rectangle}} q^{|\lambda|} = \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

So to show the result we'll count the ways that we can produce such young diagrams.

First, note that counting the ways that we can start off at $(0, n-k)$ and reach $(k, 0)$ using only steps of $(1, 0)$(East) and $(0, -1)$(South) will trace the young diagrams of these integer partitions. However, we'll do this in a flipped manner from that done in the proof of Theorem (1.9). So breaking these down into 2 distinct cases, it'll be easier to count these cases: (1.) step to the east, (2.) step to the south.

- (1.) Stepping to the east we'll get that we'll be at the point $(1, n-k)$, to then reach $(k, 0)$, this is equivalent to traversing a box of size $(k-1) \times (n-k) = (k-1) \times (n-1-k+1) = (k-1) \times (n-1-(k-1))$. By Theorem (1.9)(Mendes & Remmel) we have that this is exactly $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$.
- (2.) Stepping to the south, we'll be at the point $(0, n-k-1)$. This gives us a box of size $k \times (n-k-1) = k \times (n-1-k)$ then we know that by Theorem (1.9) there are $\begin{bmatrix} n-1 \\ k \end{bmatrix}_q$ ways to do this. But this is undercounting the Young diagrams, note that this immediately produces an "empty" row of width k and height 1 above the "filled" Young diagram. Thinking about the Young diagrams that can be produced from here on this is the complement of the "empty" Young diagram above the one we're tracing in the box of size $k \times (n-k)$. This "empty" Young diagram has a top row of size $k \times 1$.

So this gives us a minimum value of the Young diagram's going on being at least q^k. So we have a total in this case of:

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

Giving us the result. □

38.

Let q be a prime power, $\mathbb{F}_q$ be a finite field with q elements, and $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$.

a.

Prove that the number of k dimensional subspaces in $\mathbb{F}_q^n$ is equal to $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Proof. Let q be a prime power, $\mathbb{F}_q$ be a finite field with q elements, and $\mathbb{F}_q^n$ be the $n-$dimensional vector space over $\mathbb{F}_q$.

First a quick note. Suppose $q = p^k$ for some prime p and $k \in \mathbb{N}$. Then note that $[\mathbb{F}_{p^k} : \mathbb{F}_p] = k$. So that we can treat $\mathbb{F}_{p^k}$ as a vector space over the finite field $\mathbb{F}_p$. So that showing the result for $\mathbb{F}_p$ will imply the result for the field $\mathbb{F}_{p^k} = \mathbb{F}_q$.

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ with $k \leq n$ and let q be a prime number. Note that because $\mathbb{F}_q^n$ is a n-dimensional vector space over a finite field of size p, we have that their are q^n many distinct element, including $0-$vector. As we can think about $\mathbb{F}_q^n$ as the set of $n-$tuples with entries in $\mathbb{F}_q$. First, we'll count how many linearly independent sets of size k there are in $\mathbb{F}_q^n$.

So starting off with counting these, we can choose any element that isn't the 0-vector in $\mathbb{F}_n^q$, there are exactly $q^n - 1$ many choices here. Next, we need a vector that isn't a linear combination of the previous vector. Notice that since this is a single vector, any vector that isn't a scalar multiple of the previous vector will do just fine. Since our field $\mathbb{F}_q$ is of size q, there are exactly q scalar multiples of our first vector. Excluding those, we get that in total there are $q^n - q$ many choices for our second vector. In fact for $1 \leq i \leq k$, when we select the i^{th} vector in our list there will be $q^n - q^{i-1}$ many choices that leave the list linearly independent. As this vector must be not be a linear combination of the previous $i-1$ vectors. There are exactly q^{i-1} many linear combinations of $i-1$ vectors, so that we exclude all such vectors when building our linearly independent list. Finally, these choices are dependent on each other, so we must multiply to get our final total:

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{k-1}).$$

This is the total number of k-sized linearly independent lists in $\mathbb{F}_q^n$.

Now suppose we have a k-dimensional subspace of $\mathbb{F}_q^n$, to create a basis out of this there are exactly:

$$(q^k-1)(q^k-q)(q^k-q^2)\dots(q^k-q^{k-1})$$

many ways to create a basis from the elements of this subspace using the exact same reasoning as with the entire space except the size of space here is only q^k instead of q^n.

Taking any k-sized linearly independent list from $\mathbb{F}_q^n$ will then form a subspace of $\mathbb{F}_q^n$. But that basis will not be unique, so we divide by how many basis lists there are per subspace. So then we have that the number of k-dimensional subspaces of $\mathbb{F}_q^n$ is:

$$\frac{\text{Total \# of k-sized linearly independent lists of } \mathbb{F}_q^n}{\text{Total \# of basis lists for a k-dimensional subspace}}.$$

Having already solved for these we get our result after some manipulation:

$$\begin{aligned}
\text{\# of k-dimensional subspaces of } \mathbb{F}_q^n &= \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1}}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} \\
&= \frac{(q^n-1)q(q^{n-1}-1)\dots q^{k-1}(q^{n-k+1}-1)}{(q^k-1)q(q^{k-1}-1)\dots q^{k-1}(q-1)} \\
&= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} \\
&= \frac{\frac{q^n-1}{q-1}\frac{q^{n-1}-1}{q-1}\cdots\frac{q^{n-k+1}}{q-1}}{\frac{q^k-1}{q-1}\frac{q^{k-1}-1}{q-1}\cdots\frac{q-1}{q-1}} \\
&= \frac{[n]_q[n-1]_q\dots[n-(k-1)]_q}{[k]_q[k-1]_q\dots[1]_q} \\
&= \frac{[n]_q!}{[k]_q![n-k]_q!} \\
&= \begin{bmatrix} n \\ k \end{bmatrix}_q.
\end{aligned}$$

We have our result! □

b.

Let X be a vector space with a finite number of elements x. Show that there are

$$\begin{bmatrix} n \\ n-k \end{bmatrix}_q (x-q^0)\dots(x-q^{k-1})$$

linear maps $L : \mathbb{F}_q^n \to X$ which have a null space of dimension $n-k$.

Proof. Let X be a vector space with a finite number of elements x.

Note that for any linear operator $L : \mathbb{F}_q^n \to X$, L must satisfy the following: $\ker(L)$ is a subspace of $\mathbb{F}_q^n$, $\mathbf{range}(L)$ is a subspace of X, and that $\dim(\ker(L)) + \dim(\mathbf{range}(L)) = \dim(\mathbb{F}_q^n) = n$. So in counting the number of linear maps that have kernel (null space) of dimension $n-k$, we can actually treat this as taking a subspace of $\mathbb{F}_q^n$ with dimension $n-k$ sending everything in that subspace to the $0-$vector of X and then defining the operator around that. So we have by $(a.)$ that there are exactly $\begin{bmatrix} n \\ n-k \end{bmatrix}_q$ many subspaces of dimension $n-k$ in $\mathbb{F}_q^n$.

The rest of the proof is to count how many choices we have for the rest of the elements; that is what are our choices for the elements not getting mapped to 0. Well, since $\dim(\ker(L)) = n-k$, we have that $\dim(\mathbf{range}(L)) = k$. That is we have to create a subspace of size k when choosing where the rest of the elements that don't map to 0 go to through L. With this in mind, we can do this by taking a linearly independent list in $\mathbb{F}_q^n$ of size k and determining where each one of those elements can be mapped through L. So our first choice, we can send any such vector $v_0 \in \mathbb{F}_q^n$ to any vector in $L(v_0) \in X$ that isn't the 0-vector of X, so that we have $x - 1 = x - q^0$ many choices here. For our second choice, say $v_1 \in \mathbb{F}_q^n$, we must have that $L(v_1) \in X$ isn't a linear combination of $L(v_0) \in X$. So that is to say that $L(v_1) \neq cL(v_0) = L(cv_0)$ for any $c \in \mathbb{F}_q$. Well notice that there are exactly q elements in $\mathbb{F}_q^n$ that equal cv_0, so that we have a total number of choices here being $x - q^1$. In fact for $1 \leq i \leq k$ we'll have in determining where v_i can be mapped to produce a subspace in X we'll have $x - q^{i-1}$ many choices. That is $L(v_i) \neq c_0L(v_0) + c_1L(v_1) + \ldots + c_{i-1}L(v_{i-1}) = L(c_0v_0 + c_1v_1 + \ldots + c_{i-1}v_{i-1})$ for whatever choice of $c_0, c_1, \ldots, c_{i-1} \in \mathbb{F}_q$, and the total of number of these linear combinations is q^{i-1}. So that we have that we'll have

$$(x-1)(x-q)\ldots(x-q^{k-1})$$

many choices in producing the subspace $\mathbf{range}(L)$ in X such that $\dim(\ker(L)) = n-k$.

Because these are dependent and successive choices, we have a total of:

$$\begin{bmatrix} n \\ n-k \end{bmatrix}_q (x-q^0)(x-q^1)\ldots(x-q^{k-1})$$

choices for linear maps $L : \mathbb{F}_q^n \to X$ that have a null space or kernel of dimension $n-k$. $\square$

c.

By counting linear maps $L : \mathbb{F}_q^n \to X$, prove the $q-$Cauchy identity:

$$x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x - q^0) \dots (x - q^{k-1}).$$

Proof. First, note that for the right-hand side we have :

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x - q^0) \dots (x - q^{k-1}) = \sum_{k=0}^{n} \begin{bmatrix} n \\ n-k \end{bmatrix}_q (x - q^0) \dots (x - q^{k-1}),$$

because we have the symmetry in the $q-$binomial coefficient:

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

So that this is actually the total number of all linear maps: $L : \mathbb{F}_q^n \to X$, since the sum ranges over all $0 \leq k \leq n$, which corresponds to summing over the number of linear maps with kernels of dimension k.

To show the equality, we'll then make an argument that x^n is also the number of all linear maps $L : \mathbb{F}_q^n \to X$. Note that any linear map $L : \mathbb{F}_q^n \to X$ is completely determined by how a chosen basis of $\mathbb{F}_q^n$ gets sent through L; that is, how a basis $\{v_1, \dots, v_n\}$ gets sent through L determines the map. So we'll count how many ways the basis list $\{v_1, v_2, \dots, v_n\}$ can be sent through L to X. First, let $\{x_1, \dots, x_x\} = X$ be an enumeration of X. For v_1 we'll have $L(v_1) = x_1$ or x_2 or $\dots$ or x_x. So in total there are x-possibilities for how v_1 gets sent through L. Similarly, for any $1 \leq i \leq n$ we'll apply the same reasoning: For v_i we can have $L(v_i) = x_1$ or x_2 or $\dots$ or x_x, giving us in total x-possibilities here. So in total, we make this decision n-times to determine any map $L : \mathbb{F}_q^n \to X$, hence we have x^n many maps $L : \mathbb{F}_q^n \to X$.

Thus we have our result that:

$$\text{Total number of linear maps } L : \mathbb{F}_q^n \to X = x^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x - q^0) \dots (x - q^{k-1}).$$

□

d.

The identity in part *c.* has been shown true for prime powers q. How can we conclude that this identity is true for any complex number q?

Proof. Note that x^n is a n-degree polynomial, and that the right-hand side $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (x - q^0) \dots (x - q^{k-1})$ is a polynomial in x also of degree n. We'll show that this equality from $(c.)$ holds for complex q, by showing that x^n and the right-hand side agree at $n+1$ many points. Then we'll use the fact that there is a unique polynomial of degree n that fits to $n+1$ distinct points to get the equality.

Note that they definitely agree $x = 1$, since everything in the sum will be eliminate except for $\begin{bmatrix} n \\ 1 \end{bmatrix}_q = 1$ and $x^n = 1^n = 1$. We'll show that by induction for any $j \in \{1, \dots, n\}$ that $q^{jn} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (q^j - q^0) \dots (q^j - q^{k-1})$.

Our basis holds by the previous statement.

Suppose $q^{jn} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (q^j - q^0) \dots (q^j - q^{k-1})$ for some $j \in \{1, \dots, n\}$. Then consider the following:

$$q^{jn+n} = q^n \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}_q (q^j - q^0) \dots (q^j - q^{k-1})$$

By our induction hypothesis. It can be shown that this gets our result:

$$q^{jn+n} = \sum_{k=0}^{n+1} \begin{bmatrix} n+1 \\ k \end{bmatrix}_q (q^j - q^0) \dots (q^j - q^{k-1})$$

□