18.700 Problem Set 4 solutions

For the first problems, you may use the theorem I stated in class Tuesday October 7: there is a one-to-one correspondence

\[ U \leftrightarrow \text{Row}(A) \]

between \( r \)-dimensional subspaces of \( F^n \) and \( r \times n \) reduced row-echelon matrices having exactly one pivot in each row. (That is, no rows of \( A \) are zero.)

1. (2 points) Suppose \( F = \mathbb{F}_5 \) is the field with five elements. How many one-dimensional subspaces of \( F^4 \) are there?

We have to list all the \( 1 \times 3 \) reduced row-echelon matrices with a pivot; the pivot can be in the first, second, third, or fourth entry. The corresponding matrices are

\[
\begin{pmatrix}
1, x, y, z \\
0, 1, u, v \\
0, 0, 1, w
\end{pmatrix}, \quad \begin{pmatrix}
0, 1, u, v \\
0, 0, 1, w \\
0, 0, 0, 1
\end{pmatrix}, \quad \begin{pmatrix}
1, x, y, z \\
0, 0, 0, 1
\end{pmatrix}, \quad \begin{pmatrix}
0, 0, 0, 1
\end{pmatrix}
\]

with \( x, y, z, u, v \), and \( w \) arbitrary in \( \mathbb{F}_5 \). So there are \( 5^3 = 125 \) of the first sort, \( 5^2 = 25 \) of the second, 5 of the third, and one of the fourth, for a total of 156.

2. (3 points) Suppose \( F = \mathbb{F}_q \) is the field with \( q \) elements. How many two-dimensional subspaces of \( F^4 \) are there? (The answer will be a formula depending on \( q \), something like \( e^{2q} - \sin(q) + 7 \).)

We must list the \( 2 \times 4 \) reduced row-echelon matrices with two pivots. The pivots can be in columns 1 and 2, or 1 and 3, or 1 and 4; or 2 and 3, or 2 and 4; or 3 and 4. The possibilities are

\[
\begin{pmatrix}
1 & 0 & x & y \\
0 & 1 & z & w
\end{pmatrix}, \quad \begin{pmatrix}
1 & x & 0 & y \\
0 & 0 & 1 & z
\end{pmatrix}, \quad \begin{pmatrix}
1 & x & y & 0 \\
0 & 0 & 0 & 1
\end{pmatrix};
\]

\[
\begin{pmatrix}
0 & 1 & 0 & x \\
0 & 0 & 1 & z
\end{pmatrix}, \quad \begin{pmatrix}
0 & 1 & x & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}, \quad \begin{pmatrix}
0 & 0 & 1 & 0
\end{pmatrix}; \quad \begin{pmatrix}
0 & 0 & 0 & 1
\end{pmatrix}.
\]

For each type the variables \( x, y, ... \) can be arbitrary in \( F \), so the number of possibilities of each type is \( q \) to the number of variables. The total is therefore

\[
(q^4 + q^3 + q^2) + (q^2 + q) + 1 = q^4 + q^3 + 2q^2 + q + 1
\]

\[
= (q^2 + q + 1)(q^2 + 1)
\]

\[
= \frac{(q^3 + q^2 + q + 1)(q^2 + q + 1)}{(q + 1)(1)}.
\]

Either of the first two formulas on the right is fine as an answer. The last formula is what is called a “\( q \)-analogue” of the binomial coefficient

\[
\binom{4}{2} = \frac{4 \cdot 3}{2 \cdot 1},
\]

in the sense that the polynomial \( q^3 + q^2 + q + 1 \) is equal to 4 when \( q = 1 \), \( q^2 + q + 1 \) is equal to 3 when \( q = 1 \), and so on. The whole expression is therefore called a \( q \)-binomial coefficient:

\[
\binom{4}{2}_q = \frac{(q^3 + q^2 + q + 1)(q^2 + q + 1)}{(q + 1)(1)}.\]
The general definition is
\[
\binom{n}{r}_{q} = \text{def} \frac{(q^{n-1} + \cdots + 1)(q^{n-2} + \cdots + 1) \cdots (q^{n-r} + \cdots + 1)}{(q^{r-1} + \cdots + 1) \cdots (q + 1)(1)}.
\]

It turns out that \( \binom{n}{r}_{q} \) is a polynomial in \( q \) with nonnegative integer coefficients, and that its value at a prime power \( q \) is equal to the number of \( r \)-dimensional subspaces of \( \mathbb{F}_{q}^{n} \). This is the beginning of a very large idea in combinatorics: a lot of elementary counting problems (like counting the \( r \)-element subsets of an \( n \)-element set) have "\( q \)-analogues" which are related to linear algebra over the field \( \mathbb{F}_{q} \). Another way to say this is that linear algebra "over the field with one element" (which doesn’t really make sense) is basic combinatorics.

3. (6 points) Still assume \( F = \mathbb{F}_{q} \).

a) Suppose \( r \leq n \). Explain why the number of \( r \)-element linear independent lists \((v_1, \ldots, v_r)\) in \( F^n \) is equal to
\[
(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{r-1}).
\]

For the list \((v_1)\) to be linearly independent means that \( v_1 \neq 0 \). The total number of choices is the number of nonzero element of \( F^n \), which is \( q^n - 1 \). Once \( v_1 \) is fixed, the list \((v_1, v_2)\) is linearly independent if and only if \( v_2 \) does not belong to the one-dimensional span of \( v_1 \). This rules out \( q \) vectors, so there are \( q^n - q \) choices for \( v_2 \). In the same way \((v_1, v_2, v_3)\) is linearly independent if and only if \( v_3 \) does not belong to the two-dimensional span of \( v_1 \) and \( v_2 \), which means that there are \( q^n - q^2 \) choices for \( v_3 \). Et cetera. (That is, induction on \( r \).)

b) How many invertible \( n \times n \) matrices with entries in \( F \) are there? (Hint: parts (a) and (b) have something to do with each other.)

According to the last problem set, an \( n \times n \) matrix is invertible if and only if its columns (the image of the standard basis of \( F^n \)) are a basis of \( F^n \); that is, if and only if they are linearly independent. (Then spanning is automatic since the dimension of \( F^n \) is \( n \).) So the number of invertible matrices is the number of lists of \( n \) linearly independent vectors in \( F^n \). This number was computed in part (a): it is
\[
(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).
\]

c) Suppose \( A \) is a very large random square matrix with entries in the field \( \mathbb{F}_2 \). Is there a 30% chance that \( A \) is invertible?

The total number of \( n \times n \) matrices over \( \mathbb{F}_2 \) is \( 2^n \cdot 2^n \cdots 2^n \) \( (n \text{ factors}) \). The number which are invertible is \((2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-1}) \). Therefore the fraction which are invertible is
\[
\frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-1})}{2^n \cdot 2^n \cdots 2^n} = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{2^2}\right) \cdots \left(1 - \frac{1}{2^n}\right).
\]

This fraction is the chance that a random \( n \times n \) matrix over \( \mathbb{F}_2 \) is invertible. It’s .5 if \( n = 1 \), .375 if \( n = 2 \), and .328125 if \( n = 3 \). As \( n \) increases, this fraction gets
smaller and smaller: to pass from \( n - 1 \) to \( n \), you multiply by \( \left( 1 - \frac{1}{n} \right) \), which is (a tiny bit) less than one. For \( n = 5 \), it’s

\[
\left( 1 - \frac{1}{5} \right)^5 = 0.29800415,
\]

which is less than 30%. So the answer is no. (As \( n \) goes to infinity, these probabilities converge to an interesting number which is approximately 0.288788\ldots.)

4. (3 points) Axler, page 94, exercise 5; but \( F \) is allowed to be any field, and you need to see whether the answer depends on \( F \).

The eigenvalues 1 and \(-1\), and the corresponding eigenvectors \( \{(x, x)\} \) and \( \{(y, -y)\} \) “don’t change” with \( F \); but if \( F \) has characteristic 2 (like \( \mathbb{F}_2 \)) then there is only one eigenvalue \( 1 = -1 \), and the two sets of eigenvectors become the same.

5. (3 points) Axler, page 94, exercise 7, with the same warning.

The eigenvalues are 0 and \( n \); but if \( n = 0 \) in \( F \) (that is, if the characteristic of \( F \) divides \( n \)) then there is only one eigenvalue. The eigenvectors for the eigenvalue 0 are

\[
\{(x_1, \ldots, x_n) \mid \sum x_i = 0\},
\]

an \( n - 1 \)-dimensional space; this is true for any \( F \). If \( n \neq 0 \) in \( F \), then the eigenvectors for eigenvalue \( n \) are the one-dimensional space

\[
\{(x, x, \ldots, x) \mid x \in F\}.
\]

If \( n = 0 \) in \( F \), then these are still eigenvectors (in fact they belong to the \( (n - 1) \)-dimensional space written above) but (if \( n > 2 \)) they are not all the eigenvectors.

6. (5 points) Axler, page 95, exercise 11.

Outline: if \( v \neq 0 \) and \( STv = \lambda v \), then applying \( T \) to both sides gives \( TSTv = \lambda Tv \). If \( Tv \neq 0 \), this shows that \( \lambda \) is an eigenvalue of \( TS \).

If \( Tv = 0 \), then also \( STv = 0 \), so \( \lambda = 0 \). In this case what we know is that \( \text{null}(T) \neq 0 \), and what we want to deduce is that \( \text{null}(TS) \neq 0 \). By the rank plus nullity theorem, it is equivalent to show that \( TS \) is not surjective. But we know that \( \text{null}(T) \neq 0 \), so (rank plus nullity again) \( \text{range}(T) \neq V \), so

\[
\text{range}(TS) \subset \text{range}(T) \neq V.
\]

Therefore indeed \( TS \) is not surjective, as we wished to show.