Counting subspaces

Field: set of "numbers" w/ addition, subtraction, multiplication, division

e.x. $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \ldots$ (infinite)

Finite fields: $\mathbb{Z}/p$, p prime is typical example

Eg. $p=7$, $\frac{1}{1}=1$, $\frac{1}{2}=4$, $\frac{1}{3}=5$, $\frac{1}{4}=2$, $\frac{1}{5}=3$, $\frac{1}{6}=6$

General finite fields: $q=p^k$, $k\geq 1$, p prime,

$\exists$ unique (up to isomorphism) field $\mathbb{F}_q$ of size q

Lemma. Let V be n-dim vector space / $\mathbb{F}_q$. Then $|V| = q^n$.

pf. Pick basis $v_1, \ldots v_n$ for V. Every element of V is uniquely of the form $c_1 v_1 + \cdots + c_n v_n$, $c_i \in \mathbb{F}_q$. We have bijection between V and words of length n in $\mathbb{F}_q$.

$\Rightarrow |V| = q^n$. □

Ex. How many invertible 2×2 matrices?

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ s.t. $ad-bc \neq 0$

Equivalently, $\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}$ form basis for $\mathbb{F}_q^2$

i.e., $\begin{pmatrix} a \\ c \end{pmatrix} \neq 0$ and $\begin{pmatrix} b \\ d \end{pmatrix}$ not multiple of $\begin{pmatrix} a \\ c \end{pmatrix}$

(q multiples)

q^2-1 choices

q^2-q choices

$\Rightarrow (q^2-1)(q^2-q)$ many matrices.

Let $GL_n(\mathbb{F}_q) = \{n\times n \text{ invertible matrices}\}$

Prop. # of k-tuples of linearly independent vectors $(v_1, \dots v_k)$ in an n-dimensional $\mathbb{F}_q$-vector space is

$$\prod_{i=0}^{k-1} (q^n - q^i) = (q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$$

In particular, $|GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i) = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

Pf. Choosing $(v_1, \dots v_k)$:

- v_1 is any nonzero vector — $q^n - 1$
- v_2 any vector not in $\text{Span}(v_1)$ — $q^n - q$
- v_3 any vector not in $\text{span}(v_1, v_2)$ — $q^n - q^2$
- $\vdots$
- v_i any vector not in $\text{span}(v_1, \dots, v_{i-1})$ — $q^n - q^{i-1}$

In total, get $(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$.

For $|GL_n(\mathbb{F}_q)|$, note an $n \times n$ matrix is invertible $\iff$ column vectors form a basis

□

$$Gr_k(\mathbb{F}_q^n) = \{ W \subset \mathbb{F}_q^n \mid W \text{ is } k\text{-dimensional subspace} \}$$

Grassmannian

Thm. $$|Gr_k(\mathbb{F}_q^n)| = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

Pf. Consider counting pairs $(W, (v_1, \dots v_k))$ where $W \in Gr_k(\mathbb{F}_q^n)$ and $(v_1, \dots v_k)$ basis for W.

$(v_1, \dots, v_k)$ determines W

So by last result, # pairs $= (q^n-1)(q^n-q)\cdots(q^n-q^{k-1})$

Each k-dim subspace W has $(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$ many bases, so ratio $\frac{(q^n-1)\cdots(q^n-q^{k-1})}{(q^k-1)\cdots(q^k-q^{k-1})}$ counts $|Gr_k(\mathbb{F}_q^n)|$. □

q-number $[n]_q = \frac{q^n-1}{q-1} = 1+q+\cdots+q^{n-1}$, $[n]_1 = n$

q-factorial $[n]_q! = [n]_q[n-1]_q\cdots[2]_q[1]_q$ $\quad [n]_1! = n!$

Simplification: $\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$

$$= \frac{[n]_q[n-1]_q\cdots[n-k+1]_q}{[k]_q[k-1]_q\cdots[1]_q} = \frac{[n]_q!}{[k]_q![n-k]_q!}$$

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

$\Rightarrow |Gr_k(\mathbb{F}_q^n)| = \begin{bmatrix} n \\ k \end{bmatrix}_q$

Note: $\begin{bmatrix} n \\ k \end{bmatrix}_1 = \binom{n}{k}$

Ex. $n=4, k=2$, $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{(q^4-1)(q^4-q)}{(q^2-1)(q-1)} = 1+q+2q^2+q^3+q^4$

At $q=1$, get $6 = \binom{4}{2}$.

Is $\begin{bmatrix} n \\ k \end{bmatrix}_q$ a polynomial in q in general?

Represent k-dim subspaces as the row space of a full rank $k \times n$ matrix. Not unique, but we can get unique representative by using reduced row-echelon form

Ex. $k=2$, $n=4$. Every 2-dim subspace is row space of one of the following:

$$\begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix} \quad q^4 \quad \square\square$$

$$\begin{bmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix} \quad q^3 \quad \square\!\!\square$$

$$\begin{bmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad q^2 \quad \square\!\!\square$$

$$\begin{bmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix} \quad q^2 \quad \square\!\!\square$$

$$\begin{bmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad q \quad \square$$

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad 1 \quad \emptyset$$

$$\Rightarrow |Gr_2(\mathbb{F}_q^4)| = 1 + q + 2q^2 + q^3 + q^4$$

Each Young diagram fits inside $\square\!\!\square$

This is the Schubert decomposition of $Gr_2(\mathbb{F}_q^4)$

In general, this works: (for $Gr_k(\mathbb{F}_q^n)$)

- Reduced row echelon form has $\binom{n}{k}$ many types (look at positions of columns that have pivots)
- Given $S = \{s_1 < s_2 < \dots < s_k\}$, indices of columns, in row i, there are $n - s_i - (k-i)$ many $*$'s
  $\Rightarrow$ # of such matrices is $q^{\sum_i n - s_i - (k-i)}$
- By deleting pivot columns and reversing the rest, $*$'s form Young diagram for partition λ, which fits inside of $k \times (n-k)$ rectangle. (get bijection), and
  $\sum_i n - s_i - (k-i) = |\lambda|$.
- Hence, $|Gr_k(\mathbb{F}_q^n)| = \sum_{\lambda \subseteq k \times (n-k)} q^{|\lambda|}$.

Rmk. There is no field of size 1. However, we have

$$\lim_{q \to 1} |Gr_k(\mathbb{F}_q^n)| = \binom{n}{k}.$$

This suggests that if such a field existed, then
- $[n] = \{1, \dots, n\}$ should be an n-dim vector space over this field
- subsets are subspaces.

More info: "field with one element"

Note: if you plug in $q=1$ into formula for $|GL_n(\mathbb{F}_q)|$, get 0, so not quite q-analogue.

But if you divide out by $(q-1)^n$, and then plug in $q=1$, get $n!$.

More direct q-analogue of symmetric group:

Complete flags: $W_1 \subset W_2 \subset \dots \subset W_{n-1} \subset \mathbb{F}_q^n$

where W_i is linear subspace of dimension i.

There are $[n]_q!$ many complete flags.