Finite geometries

Finite fields

Lemma: For p prime, the ring $\mathbb{Z}/p\mathbb{Z}$ of residues mod p is a field. (Every nonzero elt has a mult. inverse)

Pf: Let $a \in \mathbb{Z}/p\mathbb{Z}$ nonzero. Then $p \nmid a$.
Consider $\{\dots, -2a, -a, 0, a, 2a, 3a, \dots\}$ (mod $p\mathbb{Z}$).
This is an additive subgroup of $\mathbb{Z}/p\mathbb{Z}$, so has order 0 or p. Since $a \neq 0$ it has order p and is the whole group. Thus $\exists k \in \mathbb{Z}$, $ka \equiv 1 \mod p$. $\square$

Thm: There is a unique finite field $\mathbb{F}_q$ of order q for all q of the form p^r for some prime p (and no other finite fields).

Construction: Formal roots of $x^q - x$ over $\mathbb{F}_p$.

Ex: $\mathbb{F}_4 = \{\text{roots of } x^4 - x\}$ as field extension of $\mathbb{F}_2$:

$= \{0, 1, \alpha, 1+\alpha\}$ where $\alpha^4 - \alpha = 0$ $\alpha \neq 0, 1$

$\Rightarrow \alpha^3 - 1 = 0$

$\Rightarrow \alpha^2 + \alpha + 1 = 0$

Note $(1+\alpha)^2 + (1+\alpha) + 1$

$\equiv 1 + \alpha^2 + 1 + \alpha + 1$

$\equiv 1 + \alpha + \alpha^2 = 0$ ✓

Classical geometry: Study $\mathbb{R}^n$ or $\mathbb{C}^n$ or $\mathbb{P}^n_{\mathbb{R}}$ or $\mathbb{P}^n_{\mathbb{C}}$

- Points - elements
- Hyperplanes - solutions to $a_1x_1+a_2x_2+\dots+a_nx_n=c$ (or 0 for $\mathbb{P}^{n-1}$)
- Lines - intersections of n-1 hyperplanes
- Circles - solutions to $x^2+y^2=c$

etc

Finite geometry: $\mathbb{F}_q^n$ or $\mathbb{P}^n_{\mathbb{F}_q}$.

Same equations.

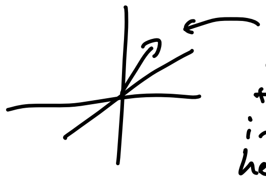
Projective space: Given a field $\mathbb{F}$,

$$\mathbb{P}^n_{\mathbb{F}} := (\mathbb{F}^{n+1}\setminus 0)/\sim$$ where $\sim$ is

the equivalence relation given by (nonzero) scalar multiplication

Ex: $\mathbb{P}^2_{\mathbb{R}} = (\mathbb{R}^3\setminus\{0\})/\sim$

$= \{(x:y:z) : x,y,z \text{ not all } 0\}$



can normalize each vector to be unit in upper hemisphere

$\uparrow$ means "homogeneous coordinates":

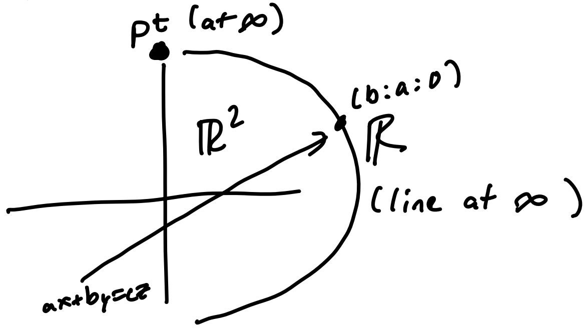
$(1:2:3)=(2:4:6)=(-1:-2:-3)=\dots$

$=(t:2t:3t)$ for any $t\in\mathbb{R}$

$\mathbb{P}^2_{\mathbb{R}}$: half sphere w/ its boundary glued to itself across origin

Normalize $z=1$ when $z\neq 0$:

$$\begin{array}{ccccccc} \mathbb{P}^2_{\mathbb{R}} = & \{(x:y:1)\} & \cup & \{(x:1:0)\} & \cup & \{(1:0:0)\} \\ & \cong & & \cong & & \cong \\ & \mathbb{R}^2 & & \mathbb{R}^1 & & pt \end{array}$$



Each pencil of parallel lines meets at a single point at ∞.

<u>Plan:</u>
- General proj space
- k-flats, counting
- Connection to matroids and designs
- SET

- Grassmannians
- Schubert cells, partitions
- Cohomology, LR rule (do chow ring)

<u>Line in $\mathbb{P}^2$:</u>

$ax+by=cz$ ("homogenization" of $ax+by=c$)

Ex: $\mathbb{P}^2_{\mathbb{F}_2} = \{\overset{①}{(0:0:1)}, \overset{③}{(0:1:0)}, \overset{⑤}{(1:0:0)}, \overset{②}{(0:1:1)}, \overset{④}{(1:1:0)}, \overset{⑥}{(1:0:1)}, \underset{⑦}{(1:1:1)}\}$

lines:

$x=0$: ①, ②, ③

$y=0$: ①, ⑤, ⑥

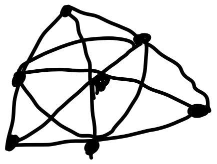
$z=0$: ③, ④, ⑤

$x+y=0$: ①, ④, ⑦

$x+z=0$: ③, ⑥, ⑦

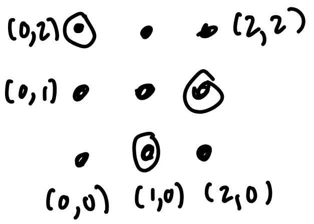
$y+z=0$: ⑤, ②, ⑦

$x+y+z=0$: ②, ④, ⑥



Fano plane!

Ex: $\mathbb{F}_3^2$:



$x + 2y = 1$

(0, 2)

(1, 0)

(2, 1)

Ex: In SET, we are looking for lines in $\mathbb{F}_3^4$.

Each dimension is an attribute:

- Color - red, green, purple
- Shape - ◇, ∿, 0
- Number - 1, 2, 3
- Shading - ○, ●, ▨

Need to find 3 cards whose attributes are either all the same or all different.

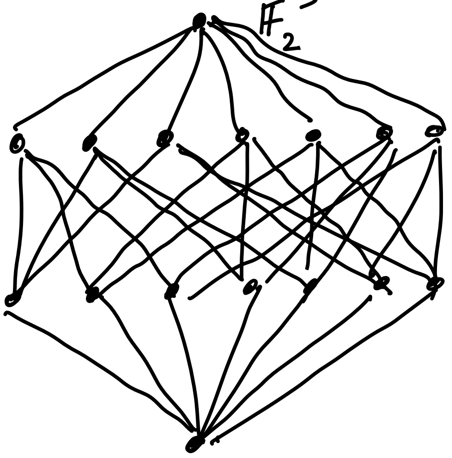
(Parameterized line: $(a,b,c,d) + t(x,y,z,w)$.

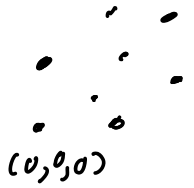
If x, y, z, or w is 0 then that attribute is "all the same". Otherwise, "all different".)

Lemma: $\mathbb{F}_q^r$ is a matroid under linear independence over $\mathbb{F}_q$, and $\mathbb{P}_{\mathbb{F}_q}^{r-1}$ is its associated simple matroid (so they have the same lattice of flats).

Pf: Loop in $\mathbb{F}_q^r$ is $\{0\}$. Parallel classes are all scalar multiples of a vector. Thus $\mathbb{P}_{\mathbb{F}_q}^{r-1}$ is the associated simple matroid. $\square$

Ex: Flats of $\mathbb{F}_2^3$: k-dim'l subspaces





$$\left.\begin{array}{l}(0,0,0\\(0,1,0)\\(1,0,1)\\(1,1,1)\end{array}\right\}\text{2-plane}$$

$$\frac{\binom{7}{2}}{\binom{3}{2}} = \frac{\frac{7\cdot 6}{2}}{3} = 7$$

$\uparrow$

#2-dim'l subspaces

Flats of $\mathbb{P}^2_{\mathbb{F}_2}$: 7 points, 7 lines (flats)

(Fano plane) ✓

Enumeration: (Hwk) How many k-flats does $\mathbb{P}^{r-1}_{\mathbb{F}_q}$ have?

Lemma: lines in $\mathbb{P}^2_{\mathbb{F}_q}$ form a 2-(v,K,λ) design, where

- $v = q^2+q+1$
- $k = q+1$
- $\lambda = 1$

Pf: Basic counting.

Lemma (Hwk): k-flats in $\mathbb{P}^{n-1}_{\mathbb{F}_q}$ form a 2-design for any fixed k.

Grassmannians: $Gr_{\mathbb{F}}(k,n) = \{k\text{-dim'l subspaces of } \mathbb{F}^n\}$

Ex: $Gr_{\mathbb{F}}(1, n+1) = \mathbb{P}^n_{\mathbb{F}}$

Analog of homogeneous coordinates:

$$Gr_{\mathbb{F}}(k,n) = \{\text{full-rank } k \times n \ \mathbb{F}\text{-matrices}\}/\sim$$

where $\sim$ is the equiv relation given by $M_1 \sim M_2$ if $\text{rowsp}(M_1) = \text{rowsp}(M_2)$.

In particular, can:

- Scale rows
- Swap rows
- Add a row to another

$\Big\}$ row reduce!

Recall: $\mathbb{P}^2_{\mathbb{R}} = Gr(1,3) = \{(1:x:y)\} \cup \{(0:1:x)\} \cup \{(0:0:1)\}$

$$Gr(2,4) = \left\{\begin{pmatrix} 1 & 0 & x & y \\ 0 & 1 & z & w \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 1 & x & 0 & y \\ 0 & 0 & 1 & z \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 1 & x & y & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\}$$

$$\cup \left\{\begin{pmatrix} 0 & 1 & 0 & x \\ 0 & 0 & 1 & y \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 1 & x & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\}$$

$\leftarrow$ "Schubert decomposition"

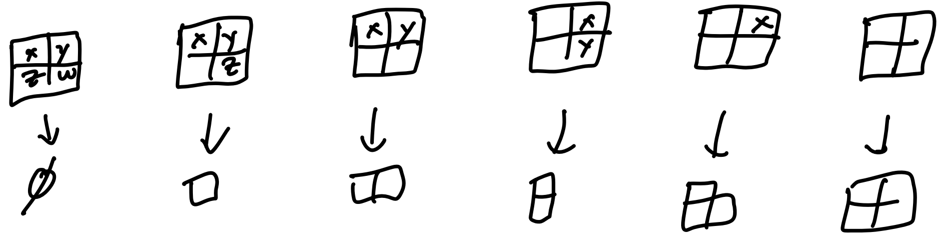
It's a 4D space over $\mathbb{F}$

Ex of row reduction to get it into a form above:

$$\begin{pmatrix}1&1&-1&3\\2&2&-1&2\end{pmatrix}\sim\begin{pmatrix}1&1&-1&3\\0&0&1&-4\end{pmatrix}\sim\begin{pmatrix}1&1&0&-1\\0&0&1&-4\end{pmatrix}$$

$$\in\left\{\begin{pmatrix}1&x&0&y\\0&0&1&z\end{pmatrix}\right\}$$

Note: the Schubert decomposition parts "cells" correspond to partitions:



= All partitions that fit in a 2×2 box!

Lemma: $Gr(k,n)=\bigcup_{\lambda\subseteq\square}\Omega^\circ_\lambda$ where $\square$ is $k\times(n-k)$

and Ω°_λ is the set of all row-reduced matrices w/ pivots in cols $\lambda_k+1,\ \lambda_{k-1}+2,\ \lambda_{k-2}+3,\ \dots,\ \lambda_1+k$

Pf: Every matrix whose rowspan is in $Gr(k,n)$ can be row reduced; the λ just keeps track of the pivot positions as above. $\square$

Enumeration over $\mathbb{F}_q$

Thm: $|Gr_{\mathbb{F}_q}(k,n)| = \binom{n}{k}_q$.

Pf: $$|Gr_{\mathbb{F}_q}(k,n)| = \sum_{\lambda \subseteq \underset{n-k}{\boxed{}}\,k} |\Omega^\circ_\lambda(\mathbb{F}_q)|$$

$$= \sum_{\lambda \subseteq \underset{n-k}{\boxed{}}\,k} q^{k(n-k)-|\lambda|}$$ ← size of complement of λ

180° rotation

$$= \sum_{\lambda \subseteq \underset{n-k}{\boxed{}}\,k} q^{|\lambda|}$$

$$= \sum_{w \in S_{0^k,1^{n-k}}} q^{inv(w)}$$

$$= \binom{n}{k}_q \qquad \square$$

Projective transformations:

$$PGL_n(\mathbb{F}) = GL_{n+1}(\mathbb{F})/\text{scaling}$$

$$= Aut(\mathbb{P}^n_{\mathbb{F}}).$$

Ex: $PGL_2(\mathbb{F}_2) = GL_3(\mathbb{F}_2)/\text{scaling}$

↑ trivial over $\mathbb{F}_2$

↑ How many invertible 3×3 matrices over $\mathbb{F}_2$?

ex. $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

$\uparrow$

- 7 choices for 1st column (not all 0)
- then, 6 choices for 2nd col (not in span of 1st col)
- First two cols span 4 vectors, so 4 choices for 3rd col

$7 \cdot 6 \cdot 4 = 168$ = size of symmetry group of Fano plane. ✓

Thm: $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$

Pf: Similar argument

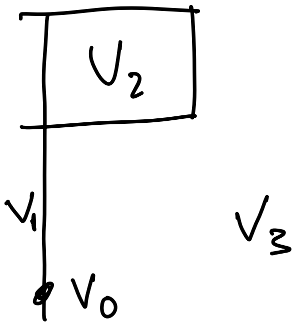
Cor: $|PGL_n(\mathbb{F}_q)| = \frac{1}{q-1}(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$

Flags

Def: A flag is a chain

$$\{0\} = V_0 \subseteq V_1 \subseteq V_2 \subseteq \cdots \subseteq V_n \subseteq \mathbb{F}^n$$

where $V_i \subseteq \mathbb{F}^n$ has dim $= i$ for all i.



<u>Enumeration</u>: How many flags in $\mathbb{F}_q^n$?

- 1 choice for V_0
- $\frac{q^n-1}{q-1}$ choices for V_1
- Choosing $V_2 \supseteq V_1$ is same as choosing a line in $\mathbb{F}_q^n/V_1$, so $\frac{q^{n-1}-1}{q-1}$ choices

⋮

- $\frac{q-1}{q-1}$ choices for V_n

$$= (n)_q \cdot (n-1)_q (n-2)_q \cdots (3)_q (2)_q (1)_q$$

$$= \boxed{(n)_q!} \text{ Flags}$$

Flag variety: $Fl_n(\mathbb{F}) = \{\text{flags in } \mathbb{F}^n\}$.

Schubert decomposition:

A flag can be represented as a list of n vectors, representing the "new direction" at each step. Put in an $n \times n$ matrix of row vectors:

$$\begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 5 \\ 0 & 2 & 1 \end{pmatrix}$$

represents
$$V_1 = sp(1 \ \ -1 \ \ 3)$$
$$V_2 = sp((1,-1,3), (2,-2,5))$$
$$V_3 = \mathbb{C}^3$$

Equivalent matrices (same flag): Can

- Scale rows
- Add a row to a <u>lower</u> row

Note: Cannot swap rows.

Row reduction algorithm to put a flag matrix in "standard form":

- Normalize top row so leftmost nonzero entry is 1

- Clear all entries below the 1 in its column
- Repeat on 2nd row and so on.

Ex:

$$\begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 5 \\ 0 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 3 \\ 0 & 0 & -1 \\ 0 & 2 & 1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & -1 & 3 \\ 0 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} \textcircled{1} & -1 & 3 \\ 0 & 0 & \textcircled{1} \\ 0 & \textcircled{1} & 0 \end{pmatrix}$$

The 1's found in each row are the pivots. Note 0's below and to left of each pivot

$\Rightarrow$ $\boxed{\text{pivots form a permutation matrix}}$

Schubert decomposition:

$$Fl_3 = \left\{\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 1 & x & y \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 1 & x \\ 1 & 0 & z \\ 0 & 0 & 1 \end{pmatrix}\right\}$$

$$\cup \left\{\begin{pmatrix} 0 & 1 & x \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right\} \cup \left\{\begin{pmatrix} 0 & 0 & 1 \\ 1 & y & 0 \\ 0 & 1 & 0 \end{pmatrix}\right\}$$

$$\cup \left\{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\right\}.$$

$$= \mathbb{F}^3 \cup \mathbb{F}^2 \cup \mathbb{F}^2 \cup \mathbb{F}^1 \cup \mathbb{F}^1 \cup pt$$

In general: define, for $\pi \in S_n$:

$X_\pi^0 = \{$flags defined by reduced matrix w/ pivots in positions $(i, \pi(i))$ for all $i\}$.

Then $\boxed{Fl_n = \bigsqcup_{\pi \in S_n} X_\pi^0}$

Lemma: $|Fl_n(\mathbb{F}_q)| = (n)_q!$

Second Proof: $|X_\pi^0(\mathbb{F}_q)| = q^{\#\text{ non-}0,1\text{ entries}} = q^{\binom{n}{2} - \mathrm{inv}(\pi)}$

ex: $\pi = 3142$

$$\left(\begin{array}{cccc} 0 & 0 & 1 & * \\ 1 & * & 0 & * \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{array}\right)\begin{array}{c} 3 \\ 1 \\ 4 \\ 2 \end{array} \qquad \left.\begin{array}{c} 3,4 \\ 1,4 \\ 1,2 \end{array}\right\} \begin{array}{l} \text{three non-inversions} \\ \binom{4}{2}-3 \text{ inversions} \end{array}$$

So
$$|Fl_n(\mathbb{F}_q)| = \sum_{\pi \in S_n} q^{\binom{n}{2} - inv(\pi)}$$

$$= \sum_{\pi \in S_n} q^{inv(rev(\pi))}$$

$$= \sum_{\sigma \in S_n} q^{inv(\sigma)}$$

$$= (n)_q! \qquad \square$$