Combinatorics

1/10/21

Lecture 4 Finite projective spaces & designs.

We "factored" the polynomial $x^{p^r-1}-1$ over $GF(p)$.
Cyclotomic coset; the set $\{0,1,\dots,p^r-1\}$ is partitioned into union of cyclotomic coset, each one giving an irr. factor of $x^{p^r-1}-1$.

1. → Introduce the concept of projective spaces.
2. → To do some computations over finite fields
3. → Generalise 1&2 into "designs".

---

1. Projective spaces.

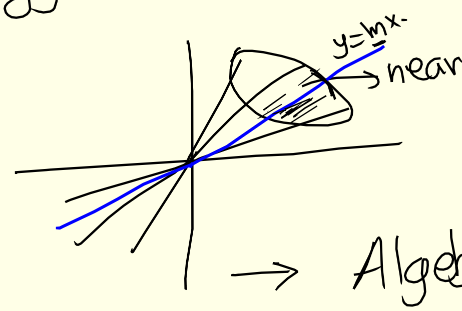
Let F be a field. V be an $n+1$-dimensional vector space over F.

$\mathbb{P}^n(F) = \{$ all one dimensional subspaces of $V\}$.

(r-dimensional Grassmannian by
$Gr(n,r,F) = \{$all r-dimensional subspaces of $V\}$)

$x \in \mathbb{P}^n(\mathbb{F})$ is a 1-dim^l subspace of V^{n+1}.

Nice topology can be introduced on this set.



If $F=\mathbb{R}$, $\mathbb{P}^n(\mathbb{R})$ is compact top. space.

→ Algebraic Geometry, we introduce Zariski topology by declaring closed sets.

Zariski Topology

Given a homogeneous polynomial in $n+1$ variables over F

$x_1^2 + x_2^1 x_3^1 + x_4^2$.

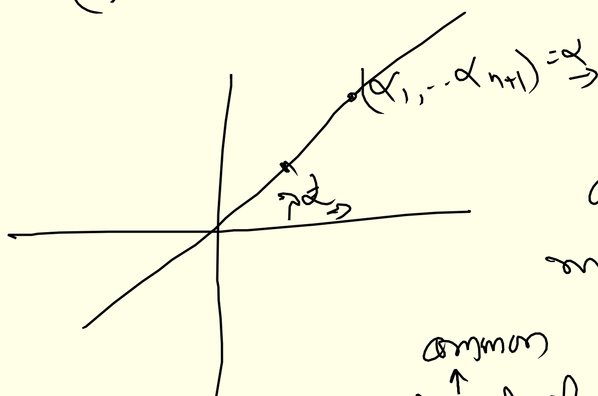
$x_1^3 + x_1 x_2$ – not homog.

$$\underset{\substack{\text{finite sum} \\ \text{over } (\mathbb{N}\cup\{0\})^{n+1}}}{\sum} a_{i_1 i_2 \cdots i_{n+1}} \underbrace{x_1^{i_1} x_2^{i_2} \cdots x_{n+1}^{i_{n+1}}}_{\text{monomial}} \quad \text{with } i_1+i_2+\cdots+i_{n+1} = M.$$

If $(\alpha_1, \alpha_2, \ldots \alpha_{n+1}) \in F^{n+1}$ is such that

$$\sum a_{i_1 i_2 \cdots i_{n+1}} \alpha_1^{i_1} \cdots \alpha_{n+1}^{i_{n+1}} = 0 .$$

then $(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_{n+1})$ is also a zero of that poly.

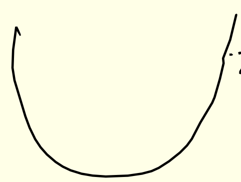


$\Rightarrow$ the set of zeroes of a homog. poly in $n+1$ variables makes sense in $\mathbb{P}^n(F)$.

$\tau = \{ C \mid C$ is the common set of zeroes of a finite set of homog. poly in $n+1$-variables $\}$

$\|$

Zariski topology. $\to$ Open sets are very big!



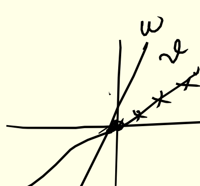
$zy = x^2$ in $\mathbb{P}^2$.

its compliment is open.

$\therefore$ This topology not Hausdorff.

Restrict our attention to $GF(q)$ where $q = p^m$ for some prime p & $m \in \mathbb{N}$.

elts in $n+1$ diml v-space over $GF(q)$ is q^{n+1}.



$q^{n+1} - 1$

1-diml subspaces $= \dfrac{q^{n+1} - 1}{q - 1}$.

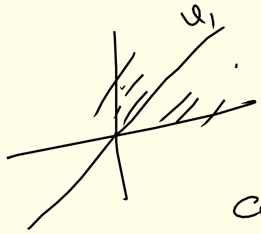
r-diml subspaces ?

Any r-diml subspace is gen by a basis $(v_1, \dots, v_r)$ with $v_1 \neq 0$; $v_2 \notin \langle v_1 \rangle$; $v_3 \notin \langle v_1, v_2 \rangle$ & so on..

v_1's $= q^{n+1} - 1$.

v_2's, given v_1 $= q^{n+1} - q$

v_3's, given v_1 & v_2 $= q^{n+1} - q^2$



$\Rightarrow$ total no. ordered lin. ind. subsets of card. r in $GF(q)^{n+1}$ is $(q^{n+1}-1)(q^{n+1}-q)(q^{n+1}-q^2)\cdots(q^{n+1}-q^{r-1})$.

Same logic tells us that # bases of an r-diml ~~ve~~ space over $GF(q)$ is

$$(q^r-1)(q^r-q)\cdots(q^r-q^{r-1}).$$

r-diml subspaces of $(GF(q))^{n+1}$
=
$\Rightarrow$ cardinality of r-diml Grassmannian is

$$\frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})}.$$

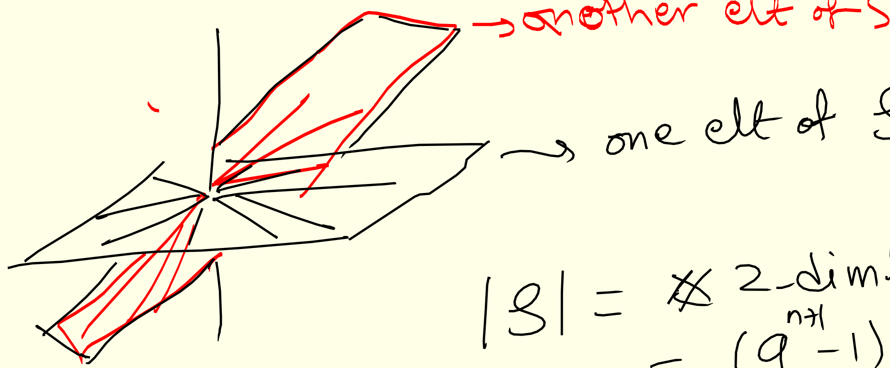
Apply this to 2-dimensional subspaces.

$$\# \text{ 2-diml subspaces} = \frac{(q^{n+1}-1)(q^{n+1}-q)}{(q^2-1)(q^2-q)}.$$

Look at $\mathbb{P}^n(GF(q)) = \frac{(q^{n+1}-1)}{q-1} = (1+q+q^2+\cdots+q^n)$
=
Look at the set of subsets of this set obtained as follows:

$$\mathcal{S} = \left\{ L_W \;\middle|\; \begin{array}{l} W - \text{2-diml subspace} \\ L_W = \{ W_1 \subset W \,/\, \dim W_1 = 1 \} \end{array} \right\}$$

ie $\mathcal{S}$ is the collection of subsets of $\mathbb{P}^n(GF(q))$ whose every element is "set of all 1-diml subspaces in a 2-diml subspace."



$|S| = \#$ 2-diml subspaces

$= \dfrac{(q^{n+1}-1)(q^{n+1}-q)}{(q^2-1)(q^2-q)}$

Each elt of S contains $\dfrac{(q^2-1)}{(q-1)} = q+1$ points of $\mathbb{P}^n(GF(q))$.

<u>example</u>. If $n=2$, then we call $\mathbb{P}^2(GF(q))$ a projective plane. In this case the no. of pts

$= \dfrac{(q^3-1)}{q-1} = 1+q+q^2.$

Also the no. of 2-diml subspaces is

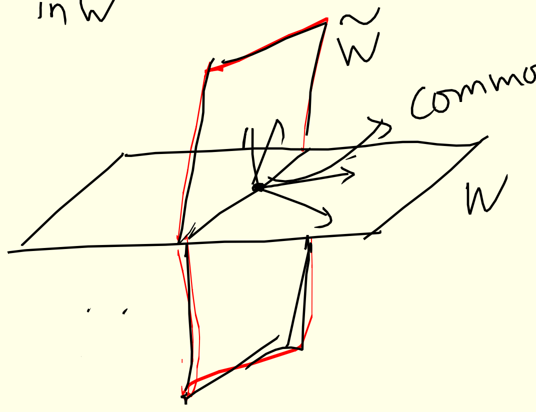
$\dfrac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} = \dfrac{\cancel{q}\cancel{(q^2-1)}\cancel{(q-1)}(1+q+q^2)}{\cancel{(q^2-1)}\ \cancel{q}\cancel{(q-1)}}$

$= 1+q+q^2 \quad =$ no. of points !

<u>Fact</u>: Moreover any two elements in S for $\mathbb{P}^2(GF(q))$ have exactly one element in common.

<u>proof</u> :- L_W & $L_{\tilde{W}}$ be two elements of S.

L_W = all 1dim. in W; $L_{\tilde{W}}$ = all 1-dim subsp in $\tilde{W}$. $W, \tilde{W}$ are 2-dim. subsp. of $(GF(q))^3$



In an l-dim v-space, the max. lin. ind. subset has cardinality l. $\Rightarrow$ $W \cap \tilde{W}$ has dim ≥ 1
& hence $= 1$.

$\boxed{3 = 2+1}$

—x—

$\boxed{\begin{array}{l} \text{Elements of } \mathcal{S} \text{ are called lines} - L_W \\ \text{Elements of } \mathbb{P}^2(GF(q)) \text{ are called points.} \\ \text{Every line contains } \frac{q^2-1}{q-1} = 1+q \text{ points.} \\ \#\text{pts} = \#\text{lines} = 1+q+q^2. \end{array}}$

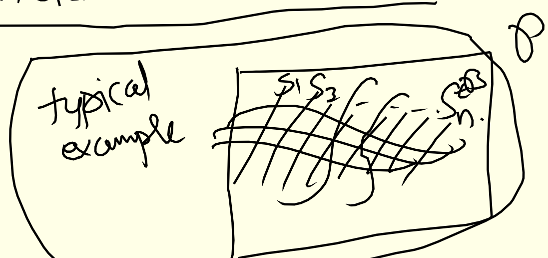
↳ projective plane over $GF(q)$.

End of part 1.

—x—x—x—

Designs (Ref. Chapter 19. A course in Combinatorics van Lint & Wilson)

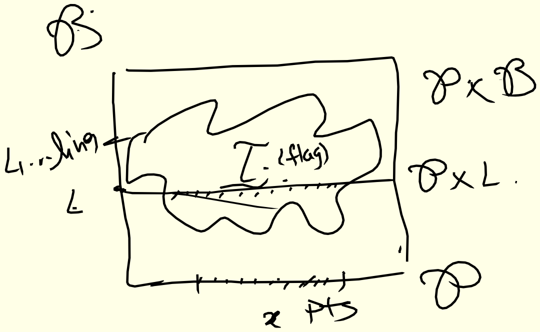
Incidence Structure. An incidence structure is a triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ where



① $\mathcal{P}$ is a set whose elts are called points.

② $\mathcal{B}$ is a set whose elts are called lines

③ $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ an incidence relation whose elements are called flags.



$(x, L) \in \mathcal{I}$ then we say that x is incident with L.
where $x \in \mathcal{P}$, $L \in \mathcal{B}$.

given $L \in \mathcal{B}$ look at all $x \in \mathcal{P}$ s.t. $(x, L) \in \mathcal{I}$.

then we get a subset of $\mathcal{P}$ corresponding to L.

In this way we can change L to a subset of $\mathcal{P}$

namely, $L \xmapsto{\theta} \{x \in \mathcal{P} \mid (x, L) \in I\}$

This gives us a map $L \to$ the set of subsets of $\mathcal{P}$.

The problem in thinking L as a subset of $\mathcal{P}$ is that θ need not be one-one. i.e. same subset may occur as images of two (or more) diff. elements of $\mathcal{B}$.

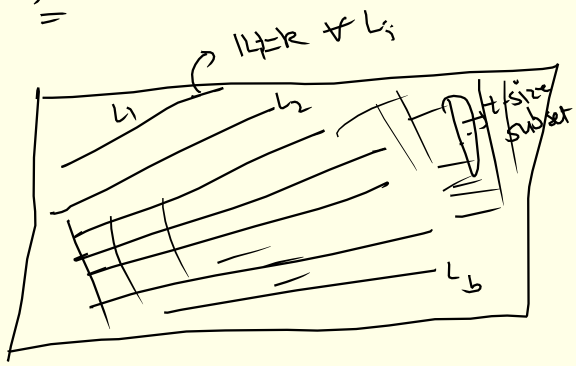
→ In this way we can think of $\mathcal{B}$ as a "collection" of elements of power set of $\mathcal{P}$ (i.e set of subsets of $\mathcal{P}$) & incidence structure becomes inclusion i.e.

$$(x, L) \in I \text{ iff } x \in L.$$

A t-design is an example of incidence structure.

∴ A t-design consists of a set $\mathcal{P}$, a collection of subsets of $\mathcal{P}$ with strong restrictions on the collection of subsets.

<u>Def^n</u> :- Let $\mathcal{P}$ be a set of <u>v</u>-elements & $\mathcal{B}$ be a collection of subsets with each elt of $\mathcal{B}$ having <u>k</u> elements such that every <u>t</u>-subset of $\mathcal{P}$ occurs in exactly <u>λ</u> elements of $\mathcal{B}$.



$\mathcal{P}$ $|\mathcal{P}| = v$.

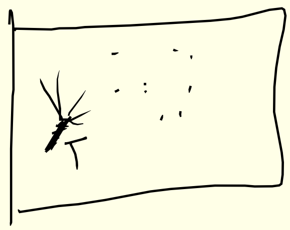
"serious" Group theory.

Then the tuple $(\mathcal{P}, \mathcal{B})$ is called a t-design denoted by $S_\lambda(t, k, v)$ with $1 \le t \le k \le v$.

↳ repetition factor

Remark. $\boxed{\text{trivial design}}$ $\mathcal{P}$ any set of size v
& $\mathcal{B} =$ all sets of size k.

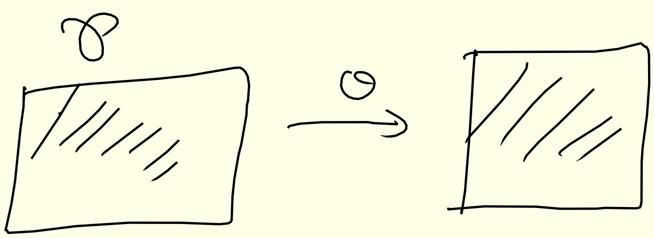
Any t-subset can be extended to a k-subset in



$\binom{v-t}{k-t}$ ways

$\Rightarrow \lambda =$ repetition no $= \binom{v-t}{k-t}$.

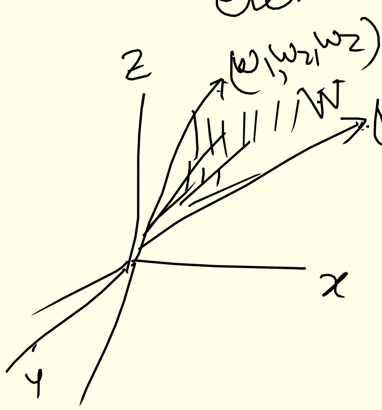
Def^n. Automorphism of a t-design $\mathcal{D}$.
is a 1-1 (onto) map $\theta : \mathcal{P} \to \mathcal{P}$ s.t.
$\theta(L) \in \mathcal{B}\ \forall L \in \mathcal{B}$.
i.e. If $x \in L \Rightarrow \theta(x) \in \theta(L) \in \mathcal{B}$.



set of auto. of trivial design $= S_v$ the perm. grp on v-letters.

(2) $\mathbb{P}^2(GF(q)) = \mathcal{P}$.
$\mathcal{B}$ = All lines.

$|\mathcal{P}| = 1+q+q^2$
$L \in \mathcal{B}$ then $|L| = 1+q$.
& $t=2$ & $\lambda = 1$ i.e. Given any two distinct points, $\exists !$ element L of $\mathcal{B}$ containing both of them.



$(v_1, v_2, v_3) \in \mathbb{P}^2(GL(q))$

namely the plane W formed by those two points gives the (unique) line that contains both of them!
block

$\therefore$ $\mathbb{P}^2(GF(q))$ is $S_q(2, 1+q, 1+q+q^2)$ - design.
$\quad\;\; \overset{\shortparallel}{\lambda} \quad \overset{\shortparallel}{t} \quad \overset{\shortparallel}{k} \quad \overset{\shortparallel}{v}$

Q. Find out parameters $1 \le t \le k \le v$ & λ so that a $S_\lambda(t, k, v)$ - design exists!

—x—x—x—

Another way to restrict the defⁿ of incidence structure to a more "manageable proportion"

Linear space :- An incidence structure is called a linear space if every block contains at least two points and any two points are contained in a unique block.

(The only diff. betⁿ a linear space & a t-design is that the ~~#~~ pts in a line is not fixed.)

otherwise, $t=2, \lambda=1$. $v=|\mathcal{P}|$. is given. Only k is not fixed

Theorem (Erdős & De Bruijn - 1948)

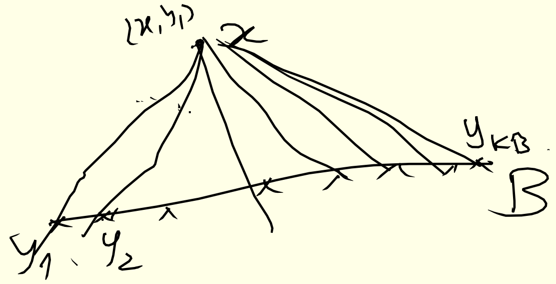
If $(\mathcal{P}, \mathcal{B}, I)$ is a linear space with $|\mathcal{B}|=b$, $|\mathcal{P}|=v$ then either $b=1$ or $b \geq v$.

(Remark: $b=1 \Rightarrow \mathcal{P}$ is the only block. $\therefore$ trivial design with $k=v=|\mathcal{P}|$.)

(Conway)

proof :- Assume $b \neq 1$.

denote by r_x the no. of blocks (they will be called lines from now on!) that contain x. Ily for $B \in \mathcal{B}$ let $k_B = |B|$.



$\Rightarrow \gamma_x \geq k_B \quad \forall x \notin B.$

Assume $b \leq v$.
(we will try to get a contradiction)

$\langle x, y_1 \rangle = \langle x, y_2 \rangle$

$\{y_1, y_2\} \subseteq B$

$\{y_1, y_2\} \subseteq \langle x, y_1 \rangle$.

$b \leq v$ & $\gamma_x \geq k_B$ $\forall x \notin B$ we must have

$bv - bk_B \geq bv - v\gamma_x \quad \forall x \notin B. \Rightarrow \frac{1}{bv - k_B} \leq \frac{1}{bv - v\gamma_x}$

$$\sum_{\substack{(x,B) \\ x \notin B}} \frac{1}{bv - v\gamma_x} \geq \sum_{\substack{(x,B) \\ x \notin B}} \frac{1}{bv - bk_B}$$

$$1 = \sum_{x \in \mathcal{P}} \sum_{\substack{B \in \mathcal{B} \\ x \notin B}} \frac{1}{v(b - \gamma_x)} \geq \sum_{B \in \mathcal{B}} \sum_{\substack{x \in \mathcal{P} \\ x \notin B}} \frac{1}{b(v - k_B)} = 1$$

Reason.

$$LHS = \sum_{x \in \mathcal{P}} \frac{1}{v} \sum_{\substack{B \in \mathcal{B} \\ x \notin B}} \frac{1}{(b - \gamma_x)}$$

Fixing x we have $b - \gamma_x$ blocks that do not contain x.

$$\Rightarrow \frac{1}{b - \gamma_x} \sum_{\substack{B \in \mathcal{B} \\ x \notin B}} 1 = \frac{b - \gamma_x}{b - \gamma_x} = 1.$$

$$\therefore LHS = \sum_{x \in \mathcal{P}} \frac{1}{v} \cdot 1 = \frac{1}{v} \sum_{x \in \mathcal{P}} 1 = 1.$$

Ily $$RHS = \sum_{B \in \mathcal{B}} \frac{1}{b} \sum_{\substack{x \in \mathcal{P} \\ x \notin B}} \frac{1}{v - k_B} = \sum_{B \in \mathcal{B}} \frac{1}{b} \left(\frac{1}{v - k_B} \sum_{x \notin B} 1 \right)$$

$$= \sum_{B \in \mathcal{B}} \frac{1}{b} \cdot 1 = 1.$$

$\Rightarrow \quad 1 = \left(\sum\sum \text{summand}_1\right) \geq \left(\sum\sum \text{sum}_2\right) = 1.$

$\Rightarrow \quad \geq$ is actually $=$.

& each summand for pair $(\alpha, B) \mid \alpha \notin B$ must be same!

$$\Rightarrow \quad \cancel{vb} - v\gamma_x = \cancel{vb} - bk_B \quad \forall x \notin B. \quad \gamma_x \geq k_B.$$

$$\Rightarrow \underline{\gamma_x = k_B \quad v = b}.$$

QED!