Mm5023 lecture 14

Finite geometry and Latin squares

Modular arithmetic

$\mathbb{Z}/m\mathbb{Z}$ quotient of $\mathbb{Z}$ by the subgroup generated by $m \in \mathbb{Z}^+$

$= \{0, 1, 2, \dots m-1\}$

$+ \quad \cdot$

$a + b = (a+b) \bmod m$

$a \cdot b = (a \cdot b) \bmod m$

It is a ring with unit 1 and trivial element 0

A **ring** (with unity) is $(R, +, \cdot, 0, 1)$ such that

$(R, +, 0)$ is an abelian group

- $\cdot$ associative
- 1 identity for $\cdot$
- Distributivity law

A **field** is a commutative ring R ($\cdot$ is commutative) in which every $u \neq 0$ has an inverse ($\exists\ v \in R$ such that

$$u \cdot v = v \cdot u = 1$$
)

Theorem: if $\mathbb{F}$ is a field and $|\mathbb{F}| < +\infty$ then $|\mathbb{F}| = p^t$ for some $t \in \mathbb{N}$.
In addition there is an irreducible degree t polynomial $q(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ such that

$$\mathbb{F} = \mathbb{Z}/p\mathbb{Z}[x] \Big/ (q(x))$$

$\mathbb{F}$ & $\mathbb{K}$ have the same size $\Rightarrow$ $\mathbb{F} \simeq \mathbb{K}$.

p prime $\quad q = p^b \quad b \in \mathbb{N}$

$\mathbb{F}_q$ is the field with q element.

Latin squares

There are 4 applicants for at a job interview
They have to perform 4 tasks
1) speak with the Dean
2) Give a research talk
3) Give a trial lecture
4) Tour the campus.

APPLICANT

	1	2	3	4
DAY 1	1	2	3	4
DAY 2	2	3	4	1
DAY 3	3	4	2	1
DAY 4	4	1	2	3

Good Schedule

No number repeat twice in row in col.

Definition A latin square of size n is a nxn matrix $(L(i,j))$ such that

1) $L(i,j) \in A$ with $|A| = n$

2) $L(i,j) \neq L(i,k)$ whenever $j \neq k$

3) $L(i,j) \neq L(k,j)$ whenever $i \neq k$.

A farmaceutical compamy has created 4 new chemicals that can be combined with 4 old excipient to give a new medicine. Want to see which combination is best.

Divide test patient into 4 groups

L latin square for the chemical

M ——————— excipient.

want all the possible pairs are tested

$$|\{(L(i), M(j))\}| = n^2$$

Definition Two latin squares L_1 L_2 orthogonal if

$$\{(a\,b) \mid a = L_1(i,j) \quad b = L_2(i,j)\} = A^2$$

The table $(L_1(i,j)\ L_2(i,j))$ is called Greco-Latin Square.

→ All the possible pairs appears.

Example

$n=2$ $\quad A=\{1,2\}$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

the possible latin square.

$\{(12)(21)(21)(12)\}| = 2 \neq 4$

No orthogonal latin square.

Example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

these are orthogonal

$$\begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix} \Rightarrow$$

Greco-Latin square

Goal Understand how many orthogonal Latin squares of order n exist and give a way to construct them

$\Leftrightarrow$ Hindsight on finite geometry.

Proposition $A = \mathbb{Z}/n\mathbb{Z}$ $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$

Then

$$L(i,j) = ai + bj \mod n$$

gives a latin square

invertible element

$\gcd(a,n) = 1 = \gcd(b,n)$

Proof

No item repeated in the row

$$\cancel{ai} + bj = \cancel{ai} + bk$$

$$\exists\, u \in \mathbb{Z}_n / n\mathbb{Z}_e^{*} \qquad ub = 1$$

$$ubj = ubk$$

$$j = k$$

For col's it is the same

$$ai + bj = ak + bj$$

$$\downarrow$$

$$k = i$$

Standard form

Define a total order on $A = \{a_1 \dots a_n\}$ a latin square is said to be in standard form if

$L(1,j) = a_j$

First row $a_1\ a_2\ a_3\ a_4 \dots a_n$

Examples

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ standard form

$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ NOT

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$ standard $\begin{pmatrix} \boxed{2\ 3\ 1} \\ 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}$ X

Reducing to standard form.

Given a latin square L you can construct from it a latin square L^* in standard form.

$$L = \begin{pmatrix} a_{i_1} & \cdots & a_{i_n} \end{pmatrix}$$

$\sigma : S_n$

$\sigma(i_1) = 1$

$\sigma(i_2) = 2$

$\sigma(i_n) = n$

$$L^{*} = \left(\sigma(L(i,j)) \right)$$

$$L(i,j) = a_k$$

$$\sigma(L(i,j)) \to a_{\sigma(k)}$$

$$L = \begin{pmatrix} \boxed{2 \quad 3 \quad 1} \\ 1 \quad 2 \quad 3 \\ 3 \quad 1 \quad 2 \end{pmatrix}$$

$$\sigma(2) = 1$$
$$\sigma(3) = 2$$
$$\sigma(1) = 3$$

$$L^{\infty} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

Proposition if L_1 and L_2 are orthogonal latin squares then L_1^* and L_2^* are orthogonal.

$\Rightarrow$ this means that it is enough to consider standard latin squares when we want orthogonal latin squares.

Theorem

There are at most $(n-1)$ standard latin squares that are pairwise orthogonal. If $n = p^t$ with p prime. Then there are exactly $(n-1)$ pairwise orthogonal latin squares in standard form.

Sketch of the proof

There are $n-1$ pairwise orthogonal latin squares when $n = p^t$

$$\mathbb{F}_n = \{ f_1 \quad \dots \quad f_n \} = A$$

$$f_1 = 0, \quad f_n = 1$$

$$\boxed{m} \in \{2 \dots n\} \rightsquigarrow f_m \in \mathbb{F}_n^*$$

Latin square

$$L^m(i,j) = f_m \cdot f_i + f_j$$

First raw $\hookrightarrow$ 0 in the first ro.

$$0 = f_1 \quad f_2 \quad f_3 \quad \cdots \quad f_n$$

$\Rightarrow$ Standard latin square.

I created $m-1$ standard latin squares

$(L^m(i,j))$ $(L^k(i,j))$

are mutually orthogonal. use that

f_m is a unit:

$(L^m(i,j), L^r(i,j)) = (L^m(i',j'), L^k(i',j'))$

$\Rightarrow i = i'$ $j = j'$

$$\left(f_m f_k + f_j \,,\; f_k f_i + f_j\right)$$

$$\Vert$$

$$\left(f_m f_{i'} + f_{j'} \,,\; f_k f_{i'} + f_{j'}\right)$$

$$\begin{cases} f_m f_i + f_j = f_m \cdot f_{i'} + f_{j'} \\ f_k f_i + f_j = f_k \cdot f_{i'} + f_{j'} \end{cases}$$

$f_m (f_i - f_{i'}) = f_{j'} - f_j$

$f_k (f_i - f_{i'}) = f_{j'} - f_j$

$f_m (f_i - f_{i'}) = f_k (f_i - f_{i'})$

if $(i = i')$ $\Rightarrow$ $f_{j'} - f_j = 0$ $\checkmark$ $j' = j$

By contradiction $i \neq i'$ $= f_m = f_k$.

$m = k$.

And if n is not a power of a prime?

$n = 6$ Brute force

No orthogonal latin square exists

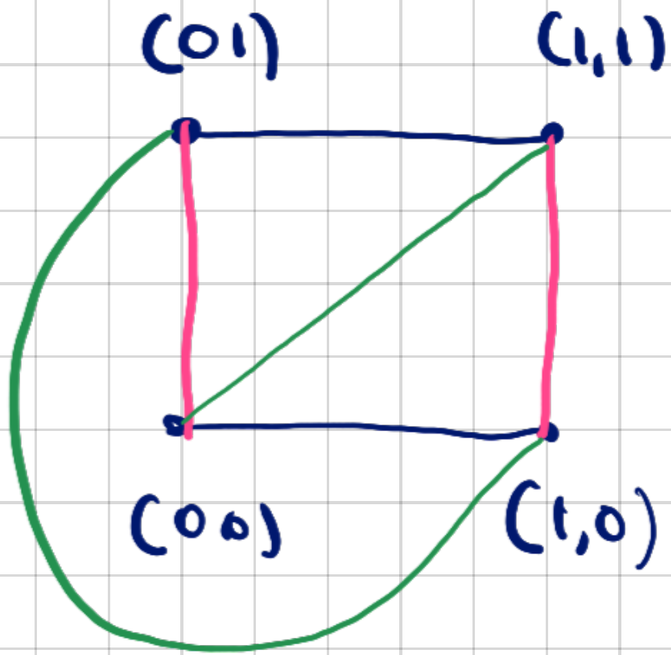
Finite affine planes. (classical Euclidean geometry) $(\mathcal{P}, \mathcal{L})$ $\mathcal{P}$ & $\mathcal{L}$ are two finite sets $\mathcal{P}$ = set of points $\mathcal{L}$ is the set of line. $l \in \mathcal{L}$ $l \subseteq \mathcal{P}$

① Given $P, Q \in \mathcal{P}$ there is a unique line $l(P, Q) \ni P, Q$

② (EUKLIDES $\vec{V}$.) Given $l \in \mathcal{L}$ $P \in \mathcal{P} \setminus l$ there is a unique line $l' \ni P$ such that $l \cap l' = \emptyset$

(3) (Non degeneracy condition) There are P_1 P_2 P_3 $P_4 \in P$ distinct no 3 on the same line.

Example



$\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$

— $x = 0$, $x = 1$

— $y = x$ $y = x + 1$

— $y = 0$ $y = 1$

Theorem $\mathbb{F}$ a finite field

$a \in \mathbb{F}$

$$L_a = \{ x = a \} \subseteq \mathbb{F}^2$$

↳ vertical lines

$a, b \in \mathbb{F}$ $L_{ab} = \{ y = ax + b \} \subseteq \mathbb{F}^2$

The pair $(\mathbb{F}^2, \{L_a, L_{ab}\})$ is a finite affine plane.

$\Rightarrow$ rank $= \sqrt{|P|} = \sqrt{n^2} = \boxed{n}$

Parallel lines

Given a finite affine plane $\Pi = (P, L)$ two lines are said to be parallel if either $l = l'$ or $l \cap l' = \emptyset$

This is an equivalence relation whose classes are called parallelity classes

Theorem : Given a finite affine plane $\Pi = (P, \mathcal{L})$ there is a natural number $\boxed{n \geq 1}$ called the ranke of Π such that

1) Every lines contains n points
2) Every point belongs to $n+1$ lines
3) There are $n+1$ parallelity classes
4) $|\mathcal{L}| = n^2 + n$
5) $|P| = n^2$

$\Pi_1 = \bigcup_{i=1}^{n} L_i \quad |\Pi| = \sum_{i=1}^{n} n = n^2$

Theorem

There is a finite plane of rank n $\Leftrightarrow$ there are $(n-1)$ mutually orthogonal standard latin squares of order n

$\Rightarrow$ New proof that there are $n-1$ MOLS of order n if $n = p^t$

Cordlary There is no affine plane of rank 6 (checked brutally for latin squares of order 6)

Proof of the existence of the rank

Lemma : every finite affine plane has at least 3 parallelity classes

Proof Non degeneracy we have P_1 P_2 P_3 P_4 three points not B on the same line.

$L(P_1P_2)$ $L(P_2P_3)$ $L(P_1P_4)$ are three distinct lines

Suppose that $L(P_1 P_i) = L(P_1 P_j)$

$P_j \in L(P_1 P_i)$ & $P_1 P_i P_j$ are on the same line $\Rightarrow$ non dég

$P_i = P_j$ $\quad$ $i = j$

All these line meet in P_1

$\Rightarrow$ they are in distinct parallelity classes.

!!

Lemma:

X finite affine plane. suppose that
a parallelity classes contains
m distinct lines then any line
not in the parallelity class contains
exactly m points

Proof

$L = \{l_1 \dots l_m\}$ parallelity class.

$l \notin L \quad l \cap l_i \neq \emptyset$

$\Rightarrow l \cap l_i = \{P_i\}$

$P_i \neq P_j$ or l_i and l_j would intersect

$\Rightarrow \mathbb{L} \ni P_1 \dots P_m \quad |L| \geq m.$

want $|L| \leq m$

(Euclides V)

$$X = \bigcup_{i=1}^{m} L_i$$

Let $P \in X$ if $P \in L_1 \Rightarrow P \in \bigcup^{m} L_i$

otherwise $\exists\, L_j \in L$ with $L_j \ni P$

$$L = L \cap X = L \cap \bigcup_{i=1}^{m} L_i = \bigcup_{1}^{n} (L \cap L_i) = \{P_i\} \quad \square$$

Proof of the theorem.

We have at least 3 parallelity classes

L_1 -
L_2
L_3

$\Big\}$ $n_i = |L_i|$

these sizes are all the same.

let l a line in L_3

$|l| = n_1$

$|l| = n_2$ $\rightarrow$ by the lemma

$n_1 = n_2$ at the same time.

$n_1 = n_3$

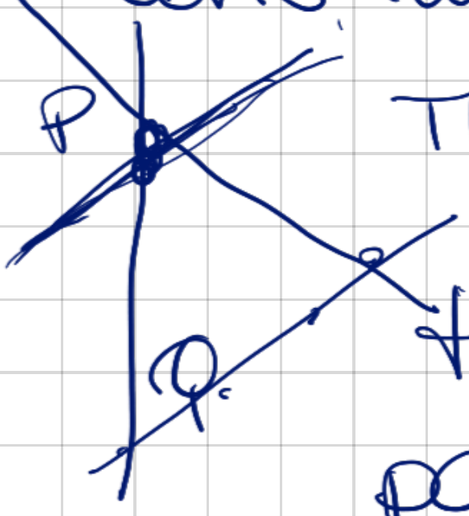
$n_3 = n_1$

$\Rightarrow$ You have at least 3 parallelity classes the are of the same size n

which also is the size of an arbitrary line in these classes

Non degeneracy $n \geq 2$.

Given a point P we want to construct $n+1$ lines through it.



There is a line through P.

there is a line $l' \parallel L$ not passing to P

For every $Q \in L'$ we have $|L'| = n$
$L(P,Q)$ give us distinct
lines thru P
$\Rightarrow \bigcup \{ L \; L(P,Q) \}$ → size $n+1$
there are at least $n+1$ lines thru P
if L'' is anotha line thru P.
then we have that eitha it is parallel
to l' or not

if yes $\Rightarrow$ $l' = C$

if no $C'' \cap C' = \{Q\}$

$l'' = C(P, Q)$