Finite Projective Planes

http://math.uwyo.edu/moorhouse/pub/planes/

Eric Moorhouse

University of Wyoming

Mutually Unbiased Bases

Let $\mathcal{B}$ and $\mathcal{B}'$ be orthonormal bases of $\mathbb{C}^n$.

We say $\mathcal{B}$ and $\mathcal{B}'$ are *unbiased* if $u^*v = \frac{1}{\sqrt{n}}$ for all $u \in \mathcal{B}$, $v \in \mathcal{B}'$.

Mutually Unbiased Bases

Let $\mathcal{B}$ and $\mathcal{B}'$ be orthonormal bases of $\mathbb{C}^n$.

We say $\mathcal{B}$ and $\mathcal{B}'$ are *unbiased* if $u^*v = \frac{1}{\sqrt{n}}$ for all $u \in \mathcal{B}$, $v \in \mathcal{B}'$.

A collection $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_d$ of orthonormal bases of $\mathbb{C}^n$ is *mutually unbiased* if any two of them are unbiased.

Mutually Unbiased Bases

Let $\mathcal{B}$ and $\mathcal{B}'$ be orthonormal bases of $\mathbb{C}^n$.

We say $\mathcal{B}$ and $\mathcal{B}'$ are *unbiased* if $u^*v = \frac{1}{\sqrt{n}}$ for all $u \in \mathcal{B}$, $v \in \mathcal{B}'$.

A collection $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_d$ of orthonormal bases of $\mathbb{C}^n$ is *mutually unbiased* if any two of them are unbiased.

It follows that $d \leq n+1$. In the case of equality, we speak of a *complete set of MUB's* (mutually unbiased bases).

Mutually Unbiased Bases

A complete set of MUB's of order $n = 2$:

$$\mathcal{B}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathcal{B}_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$\mathcal{B}_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

Each basis is represented as the columns of a unitary matrix.

Mutually Unbiased Bases

A complete set of MUB's of order $n = 3$:

$$\mathcal{B}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \mathcal{B}_2 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix},$$

$$\mathcal{B}_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega & 1 & \omega^2 \\ \omega & \omega^2 & 1 \end{bmatrix}, \quad \mathcal{B}_4 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{bmatrix}$$

where $\omega = e^{2\pi i/3}$.

Mutually Unbiased Bases

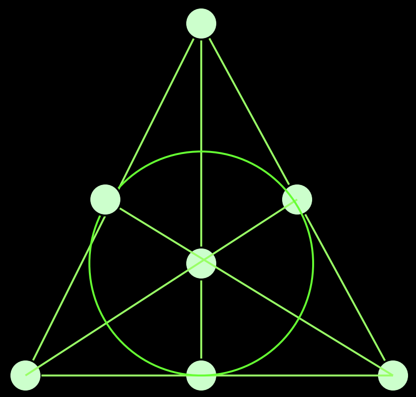
In order to have a complete set of MUB's in $\mathbb{C}^n$, must n be a prime power? (i.e. $n = p^r$, p prime, $r \geq 1$)

Projective Planes

A projective plane of order n has

- n^2+n+1 points and the same number of lines;
- $n+1$ points on each line; and
- $n+1$ lines through each point.

E.g. Plane of order $n = 2$



$n^2+n+1 = 7$ points

$n^2+n+1 = 7$ lines

$n+1 = 3$ points on each line

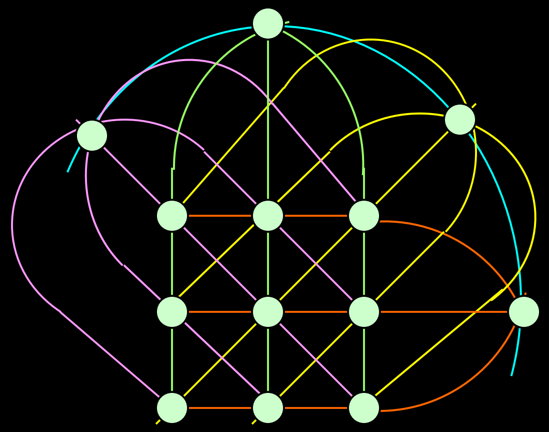
$n+1 = 3$ lines through each point

Projective Planes

A projective plane of order n has

- n^2+n+1 points and the same number of lines;
- $n+1$ points on each line; and
- $n+1$ lines through each point.

E.g. Plane of order $n = 3$



$n^2+n+1 = 13$ points

$n^2+n+1 = 13$ lines

$n+1 = 4$ points on each line

$n+1 = 4$ lines through each point

n	2	3	4	5	7	8	9	11	13
number of planes of order *n*	1	1	1	1	1	1	4	≥1	≥1

n	16	17	19	23	25	27	29	…	49
number of planes of order *n*	≥22	≥1	≥1	≥1	≥193	≥13	≥1	…	Hundreds of thousands

Nonexistence of Plane of Order 10

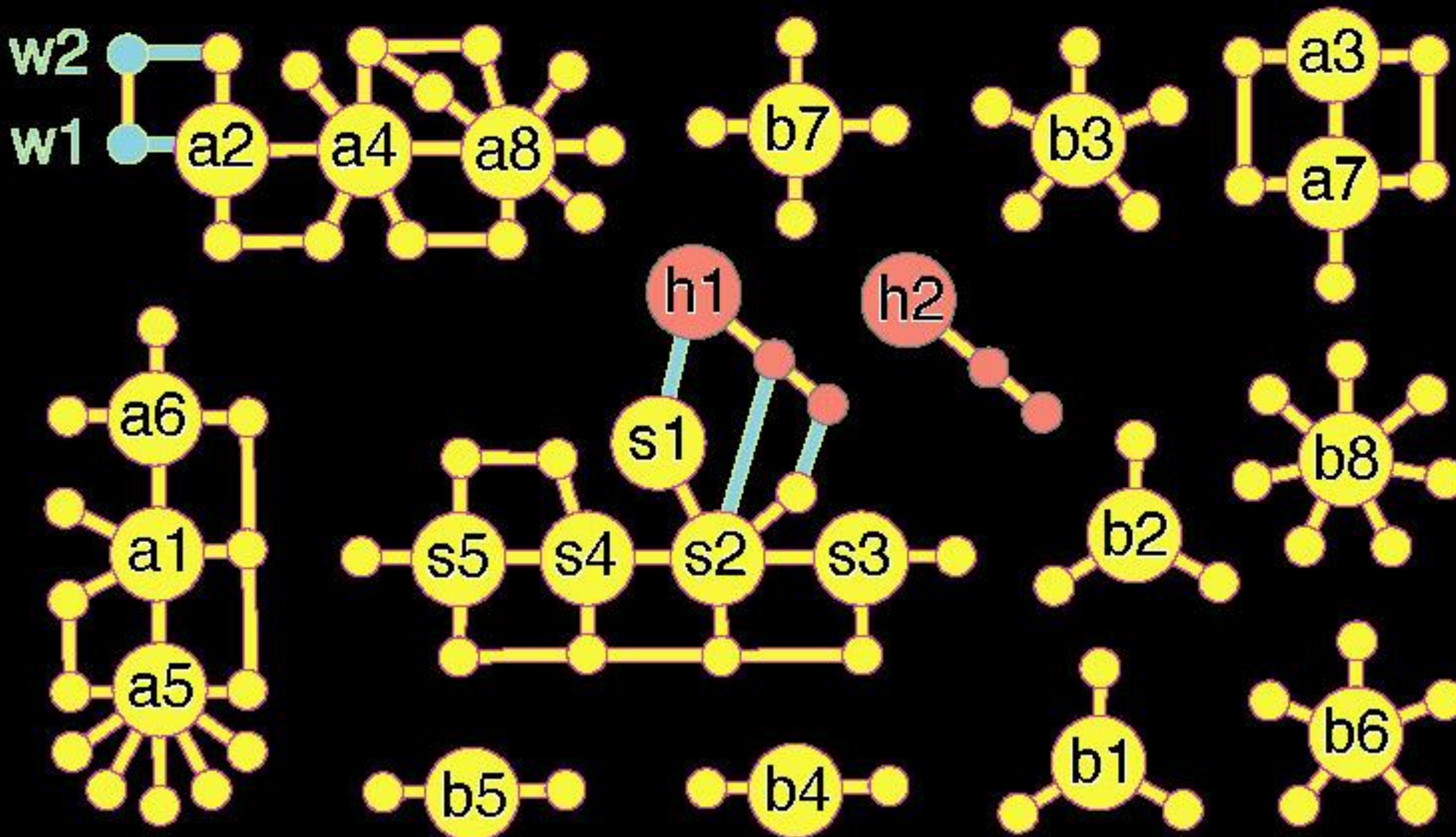
Clement Lam

Nonexistence of Plane of Order 10, c.1988

John G. Thompson

Fields Medal, 1970
Abel Prize, 2008

Known Planes of Order 25



Translation planes a1,…,a8; b1,…,b8; s1,…,s5 classified by Czerwinski & Oakden (1992)


The Wyoming Plains

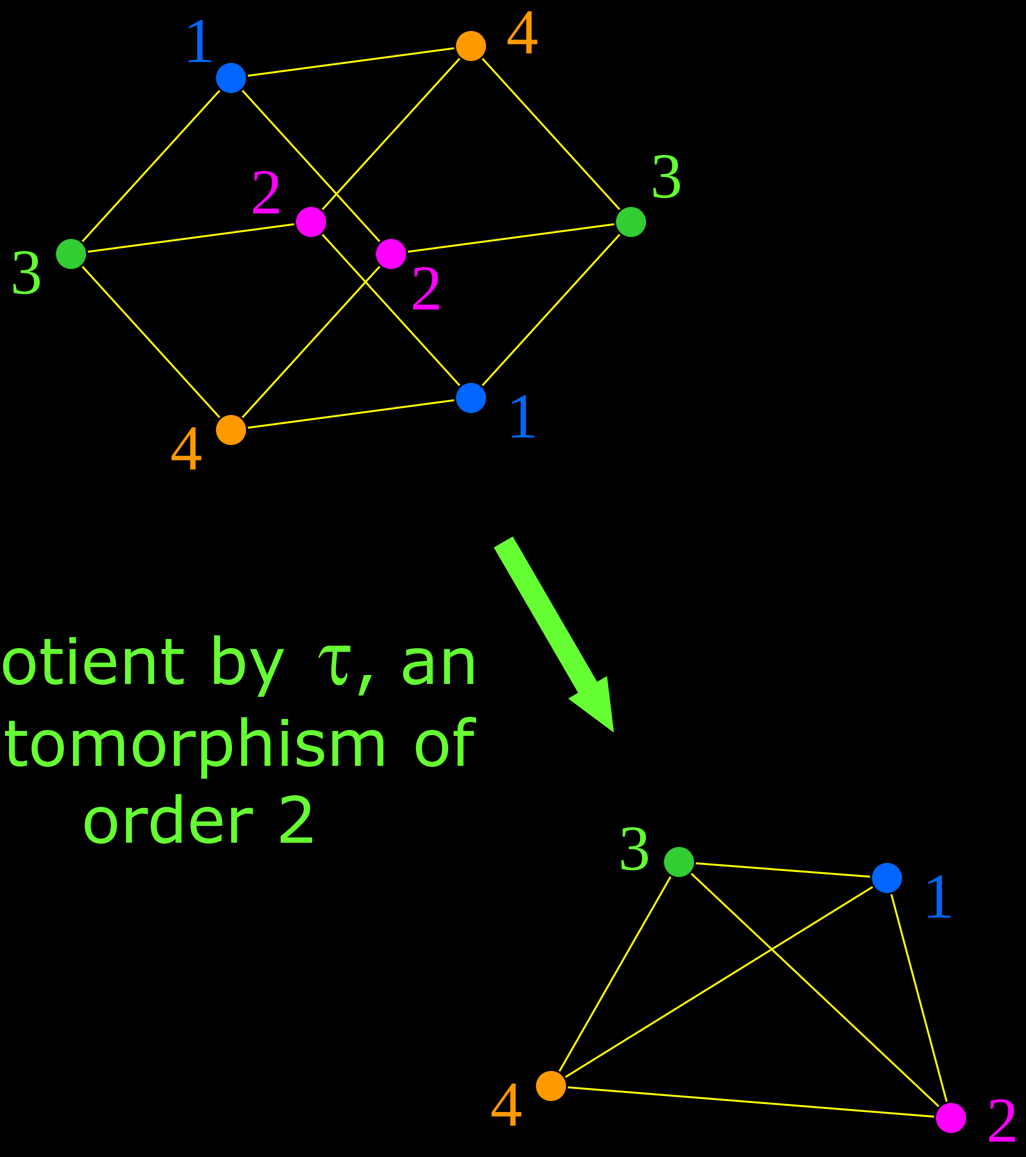
$|Aut(w1)| = 19200$

$|Aut(w2)| = 3200$

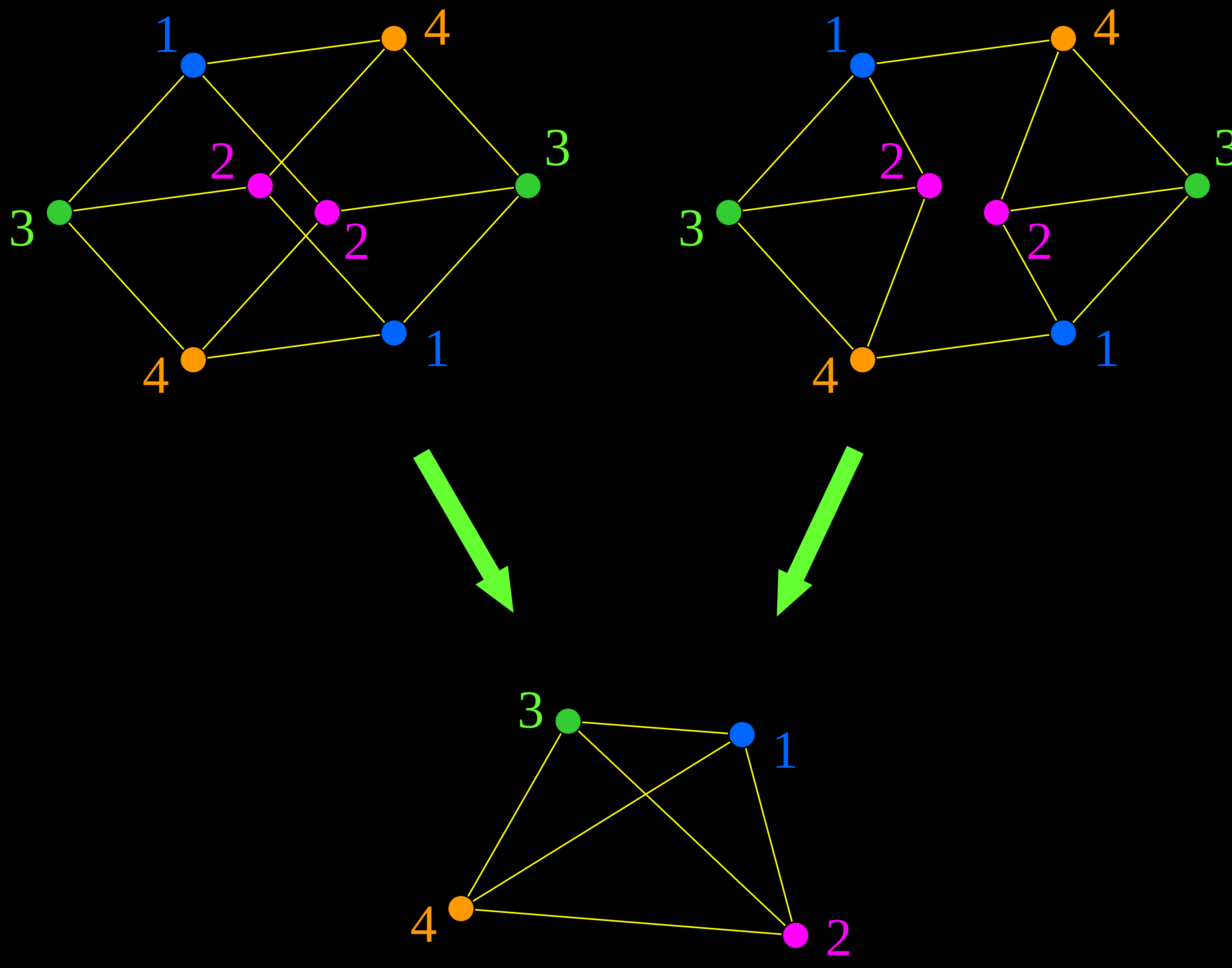
The Wyoming Planes

Thanks to my coauthor…

Where do the new planes come from?



quotient by τ, an automorphism of order 2


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

Nets

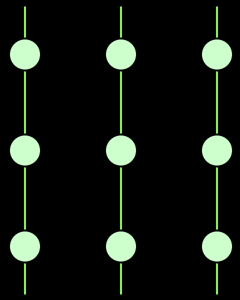
A k-net of order n has

- n^2 points;
- nk lines, each with n points.

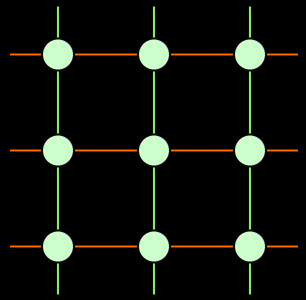
There are k parallel classes of n lines each.

Two lines from different parallel classes meet in a unique point.

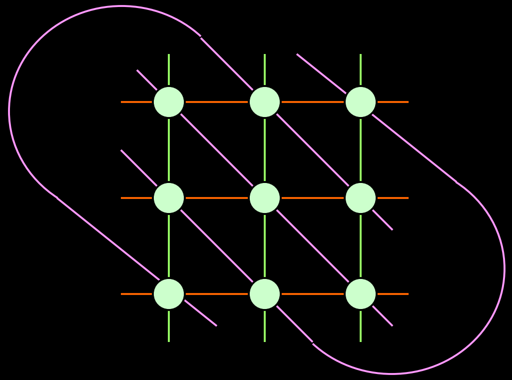
E.g. 1-net of order 3



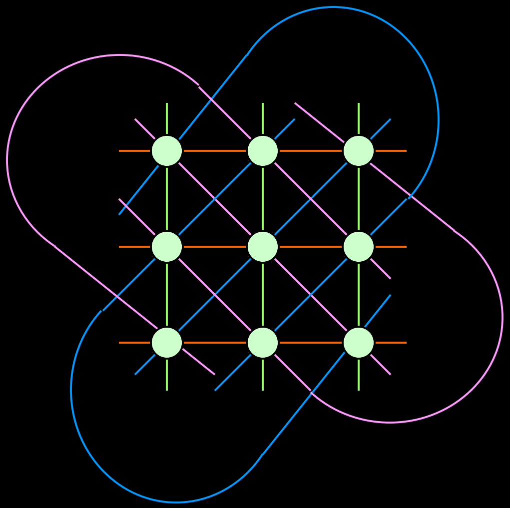
2-net of order 3



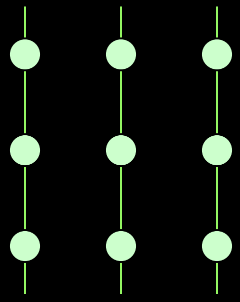
3-net of order 3



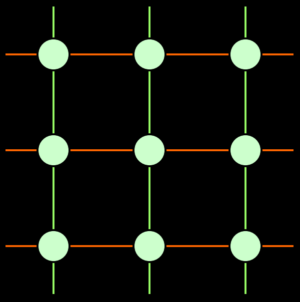
Affine plane of order 3 = 4-net of order 3



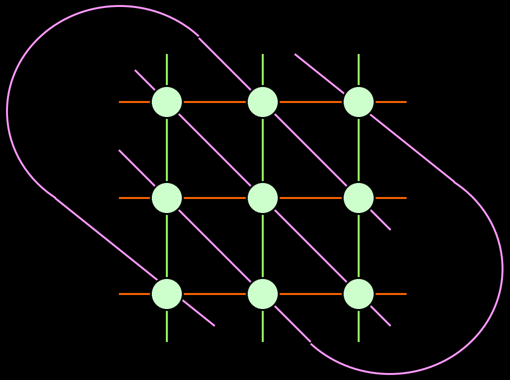
E.g. 1-net of order 3



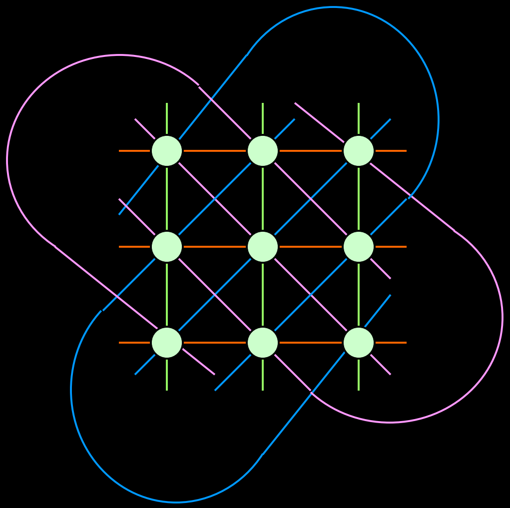
2-net of order 3



3-net of order 3



Affine plane of order 3 = 4-net of order 3



Affine plane of order n = $(n+1)$-net of order n

- n^2 points;
- $n(n+1)$ lines ($n+1$ parallel classes of n lines each).

Any 2 points are joined by exactly one line.

Any two non-parallel lines meet in a unique point.

Open Questions

1. Given an affine (or projective) plane of order n, must n be a prime power?
2. Must every affine (or projective) plane of prime order p be classical?

Affine plane of order n = $(n+1)$-net of order n

- n^2 points;
- $n(n+1)$ lines ($n+1$ parallel classes of n lines each).

Any 2 points are joined by exactly one line.

Any two non-parallel lines meet in a unique point.

Open Questions

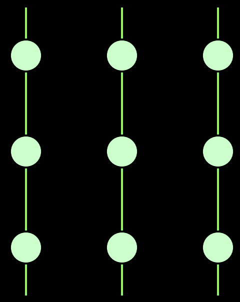
1. Given an affine (or projective) plane of order n, must n be a prime power?
2. Must every affine (or projective) plane of prime order p be classical?

One conceivable approach uses ranks of nets…

rank of a net = rank of its incidence matrix.

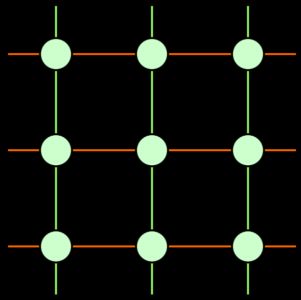
p-rank of a net = rank of its incidence matrix over $\mathbb{F}_p = \{0, 1, 2, \ldots, p\text{-}1\}$

1-net of order 3



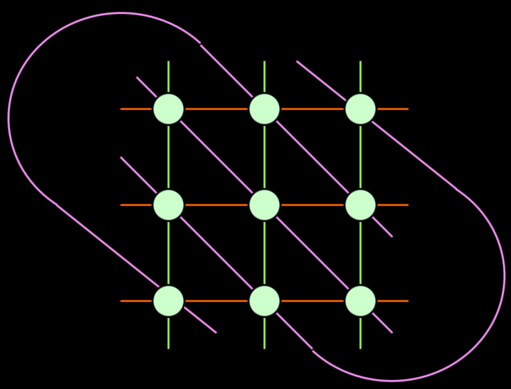
$$\mathrm{rank}_3 \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&1 \end{pmatrix} = 3$$

2-net of order 3



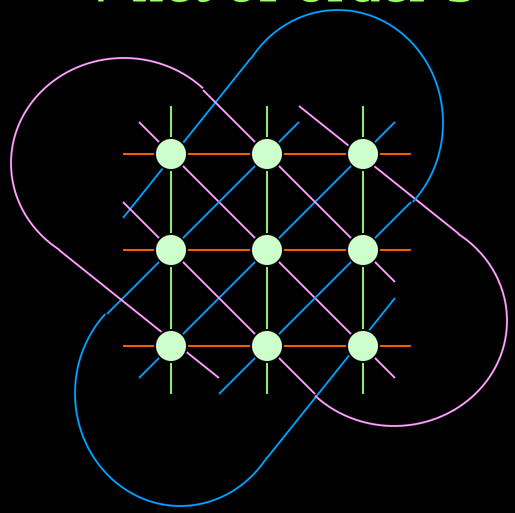
$$\mathrm{rank}_3 \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&1 \\ 1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&0&1 \end{pmatrix} = 3+2 = 5$$

3-net of order 3



$$\mathrm{rank}_3 \begin{pmatrix} 1&1&1&0&0&0&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ 0&0&0&0&0&0&1&1&1\\ 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1\\ 1&0&0&0&1&0&0&0&1\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&1&0&0&0&1&0 \end{pmatrix} = 3+2+1 = 6$$

4-net of order 3



$$\mathrm{rank}_3 \begin{pmatrix} 1\,1\,1 & 0\,0\,0 & 0\,0\,0 \\ 0\,0\,0 & 1\,1\,1 & 0\,0\,0 \\ 0\,0\,0 & 0\,0\,0 & 1\,1\,1 \\ \\ 1\,0\,0 & 1\,0\,0 & 1\,0\,0 \\ 0\,1\,0 & 0\,1\,0 & 0\,1\,0 \\ 0\,0\,1 & 0\,0\,1 & 0\,0\,1 \\ \\ 1\,0\,0 & 0\,1\,0 & 0\,0\,1 \\ 0\,1\,0 & 0\,0\,1 & 1\,0\,0 \\ 0\,0\,1 & 1\,0\,0 & 0\,1\,0 \\ \\ 1\,0\,0 & 0\,1\,0 & 0\,0\,1 \\ 0\,1\,0 & 1\,0\,0 & 0\,1\,0 \\ 0\,0\,1 & 0\,0\,1 & 1\,0\,0 \end{pmatrix} = 3+2+1+0 = 6$$

Conjecture: Any k-net of prime order p has p-rank *at least*

$$p + (p\text{-}1) + (p\text{-}2) + \dots + (p\text{-}k\text{+}1) = pk - \tfrac{1}{2}k(k\text{-}1)$$

for $k = 1, 2, 3, \dots, p\text{+}1$.

Moreover, nets whose p-rank achieves this lower bound are 'classical'.

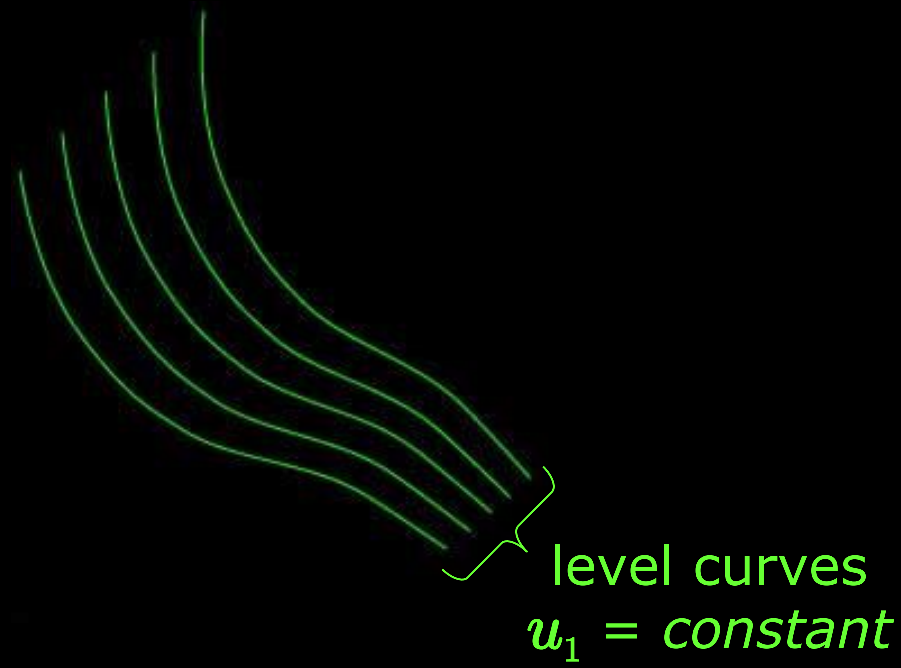
I.e. the incidence matrix of any k-net of order p has nullity *at most*

$$\tfrac{1}{2}k(k\text{-}1).$$

The corresponding statement over $\mathbb{R}$ or $\mathbb{C}$ is a theorem:

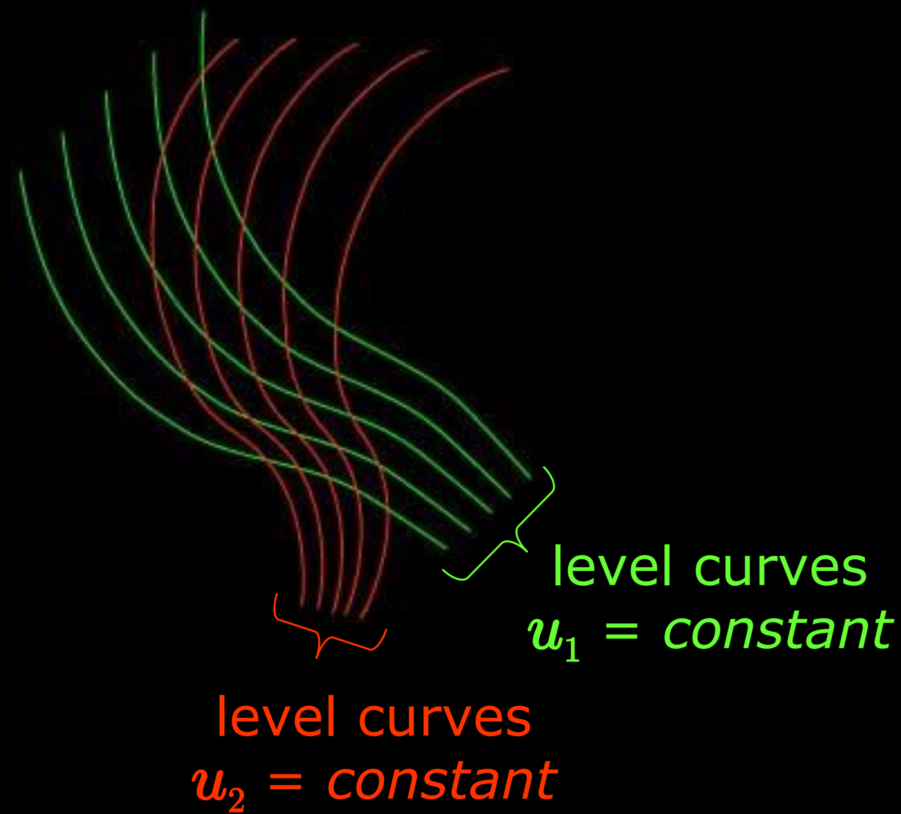
Take $F = \mathbb{R}$ or $\mathbb{C}$.

Consider functions $u_i \colon F^2 \to F$, $i = 1, 2, \ldots, k$.



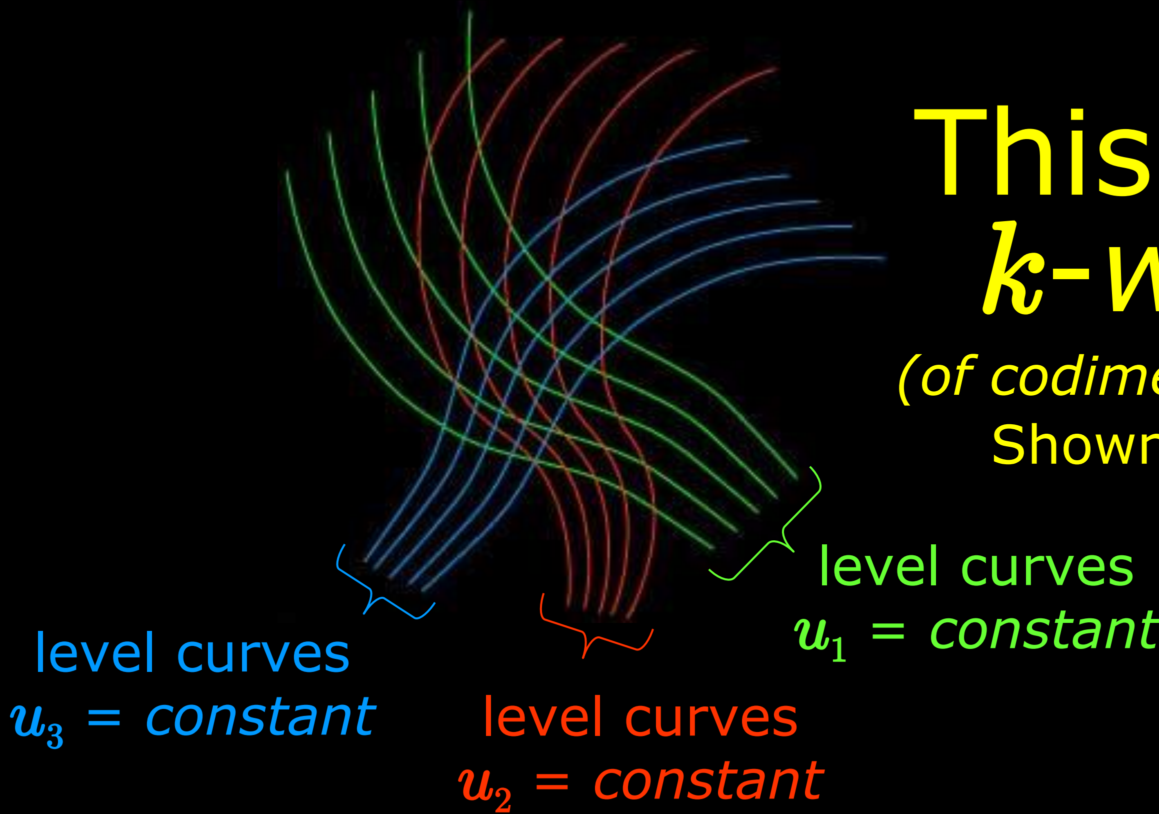
Take $F = \mathbb{R}$ or $\mathbb{C}$.

Consider functions $u_i \colon F^2 \to F$, $i = 1, 2, \ldots, k$.



Take $F = \mathbb{R}$ or $\mathbb{C}$.

Consider functions $u_i\colon F^2 \to F$, $i=1,2,\dots,k$.



This is a k-*web*
(of codimension 1).
Shown: k=3

Assume level curves meet transversely, i.e.

∇u_i, ∇u_j are linearly independent for $i \neq j$.

$F = \mathbb{R}$ or $\mathbb{C}$.

coordinate functions $u_i : F^2 \to F$, $i=1,2,\ldots,k$.

$\mathcal{V}_0$ = vector space of all k-tuples $(f_1, f_2, \ldots, f_k)$ of smooth functions $F \to F$ such that

$$f_1(u_1(P)) + f_2(u_2(P)) + \ldots + f_k(u_k(P)) = 0$$

for every point $P \in F^2$, *and* $f_i(0)=0$.

Theorem (Blaschke et al.) dim $\mathcal{V}_0 \leq \frac{1}{2}(k-1)(k-2)$.

Equality holds, e.g. in the case of `algebraic' k-webs; these arise from algebraic curves of maximal genus.

Note: dim $\mathcal{V}_0$ is called the *rank* of the k-web.

G. Bol
1906–1989

W. Blaschke & G. Bol,
Geometrie der Gewebe,
1938

W. Blaschke
1885–1962

Theorem (Blaschke et al.) dim $\mathcal{V}_0 \leq \frac{1}{2}(\boldsymbol{k}-1)(\boldsymbol{k}-2)$.
Equality holds, e.g. in the case of `algebraic' $\boldsymbol{k}$-webs; these arise from algebraic curves of maximal genus.

Note: dim $\mathcal{V}_0$ is called the *rank* of the $\boldsymbol{k}$-web.

N. Abel
1802–1829

Abel's Theorem is the foundation for the Theorem of Blaschke et al.

Chern & Griffiths:
Numerous publications on Abel's Theorem and webs

P. Griffiths
1938–

S.S. Chern
1911–2004

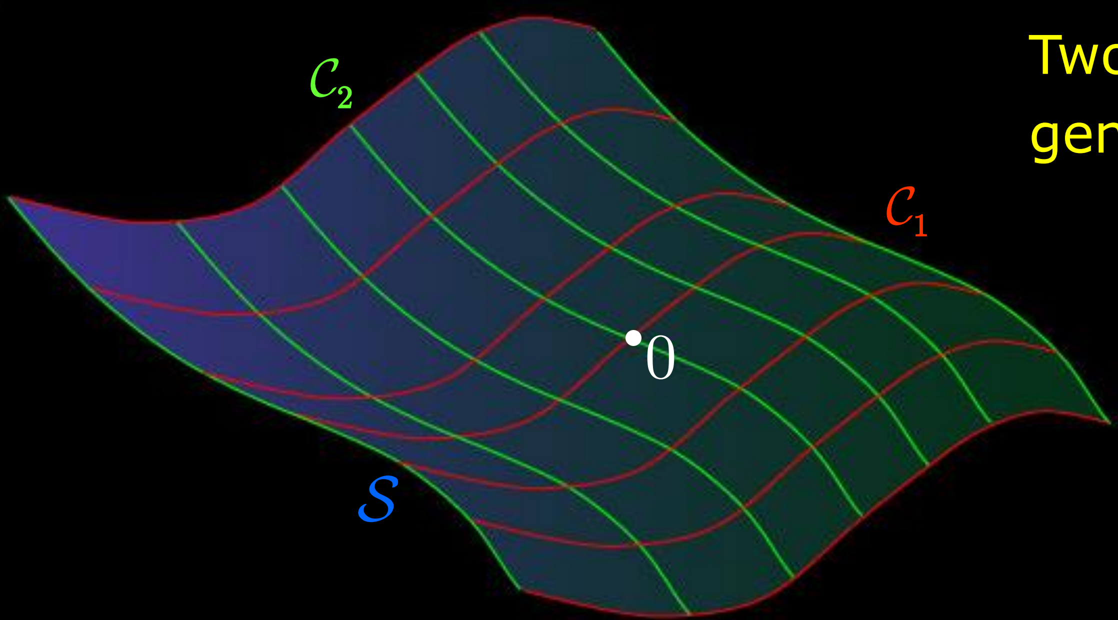
Special case $\boldsymbol{k} = 4$

A 4-*web* of rank $\boldsymbol{r}$

or

a 4-*net* of order $\boldsymbol{p}$, and $\boldsymbol{p}$-rank 4$\boldsymbol{p}$–3–$\boldsymbol{r}$

yields:



Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in $\boldsymbol{r}$-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$

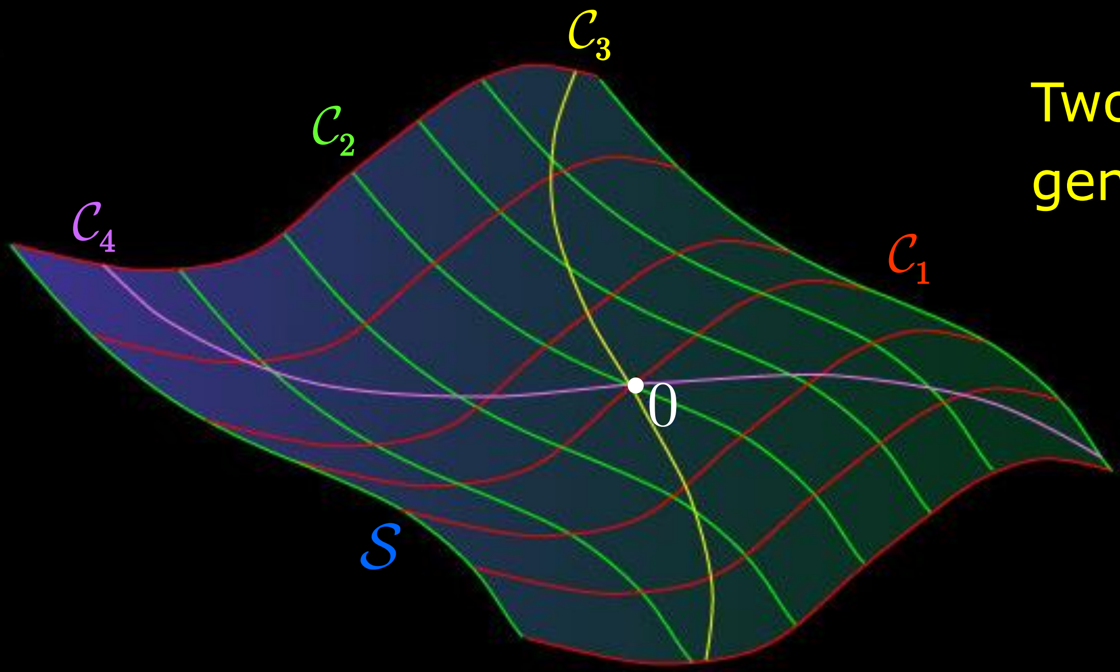
Special case $k = 4$

A 4-*web* of rank r

or

a 4-*net* of order p, and p-rank $4p$–3–r

yields:



Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in r-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$

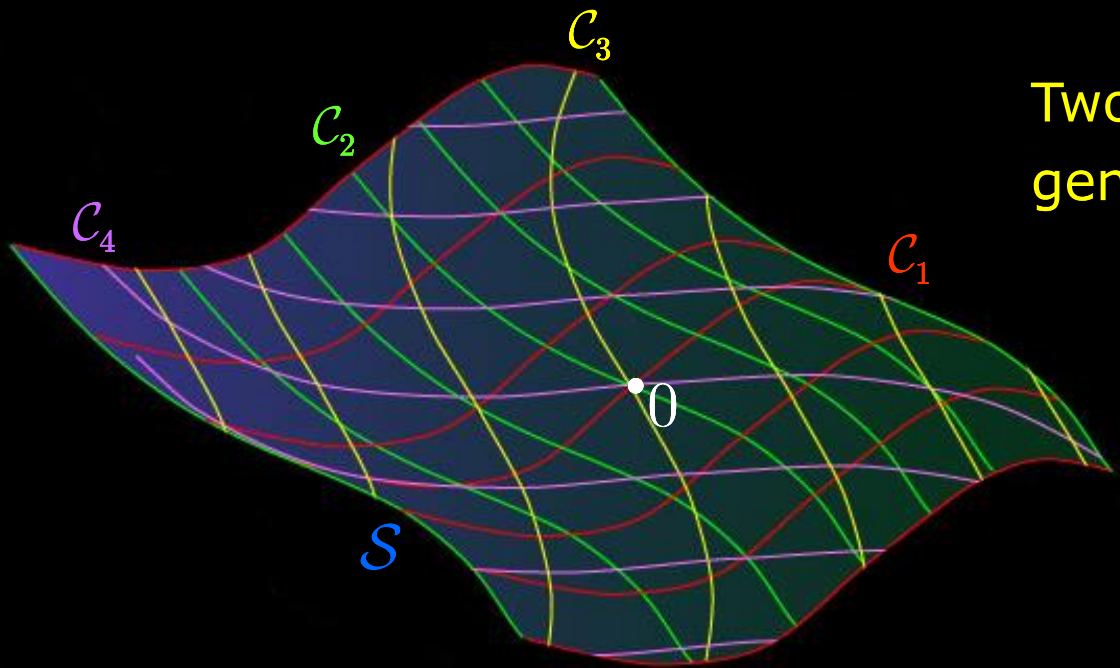
Special case $k = 4$

A 4-*web* of rank r

or

a 4-*net* of order p, and p-rank $4p-3-r$

yields:



Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in r-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$

$$= \mathcal{C}_3 + \mathcal{C}_4$$

Example

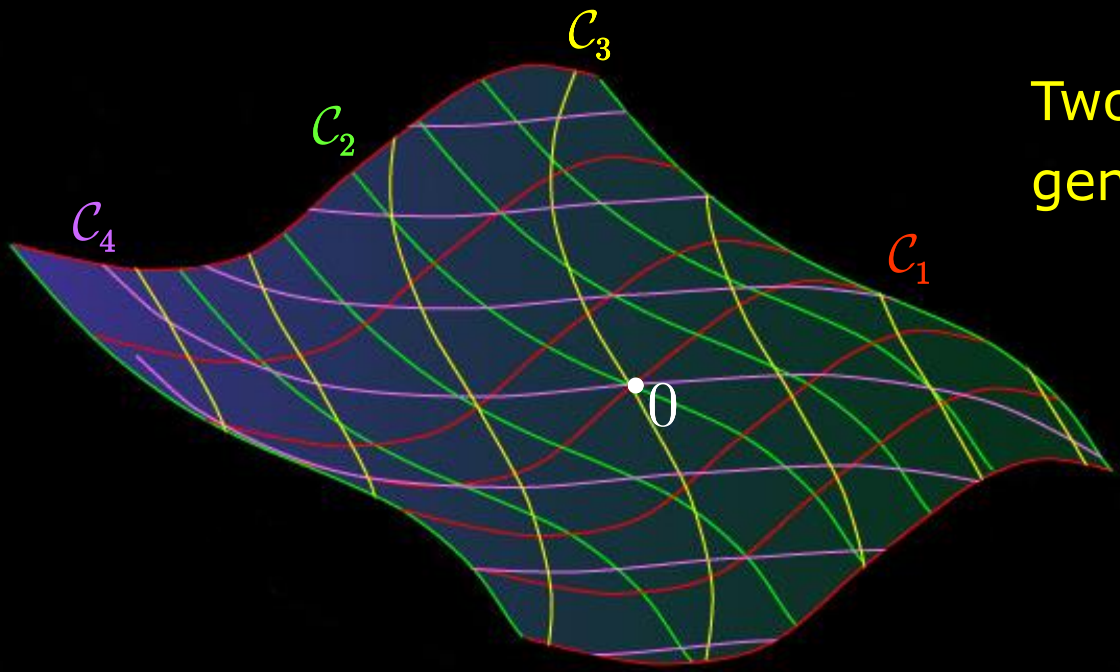
$\mathcal{S} \; : \quad z = cx^2 - y^2$

$\mathcal{C}_1 = \{(\boldsymbol{x}, 0, \boldsymbol{c}\boldsymbol{x}^2) : \boldsymbol{x} \in F\}$

$\mathcal{C}_2 = \{(0, \boldsymbol{y}, -\boldsymbol{y}^2) : \boldsymbol{y} \in F\}$

$\mathcal{C}_3 = \{(\boldsymbol{s}, \boldsymbol{cs}, \boldsymbol{c}(1-\boldsymbol{c})\boldsymbol{s}^2) : \boldsymbol{s} \in F\}$

$\mathcal{C}_4 = \{(\boldsymbol{t}, \boldsymbol{t}, (\boldsymbol{c}-1)\boldsymbol{t}^2) : \boldsymbol{t} \in F\}$



Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in 3-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$
$$= \mathcal{C}_3 + \mathcal{C}_4$$

Example 2

$\mathcal{S}$:

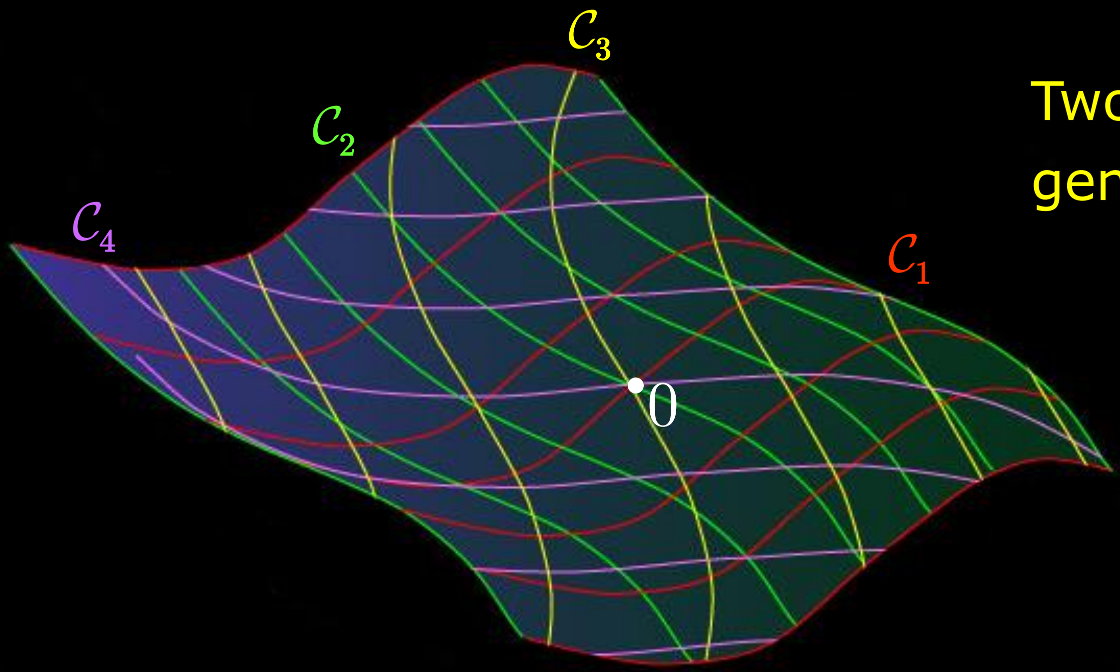
$$2z = (y+1)^4 + 2(x-1)(y+1)^2 - x^2 + 2x + 1$$

$$\mathcal{C}_1 = \{(s^2+2s, s, (s+1)^4-1) : s \in \mathbb{R}\}$$

$$\mathcal{C}_2 = \{(-2t, 0, -2t^2-2t) : t \in \mathbb{R}\}$$

$$\mathcal{C}_3 = \{(-u^2-2u, u, 1-(u+1)^4) : u \in \mathbb{R}\}$$

$$\mathcal{C}_4 = \{(-v^2, v, -v^4) : v \in \mathbb{R}\}$$

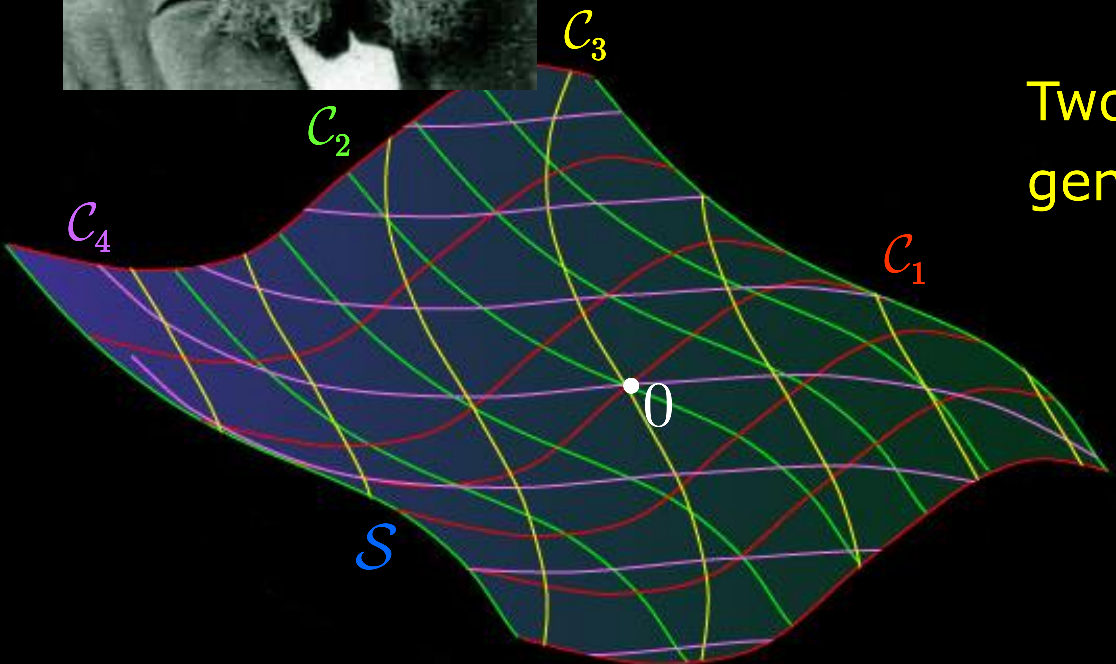


Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in 3-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$
$$= \mathcal{C}_3 + \mathcal{C}_4$$

S. Lie
1842–1899

Lie (1882) first considered such a *double translation surface.*

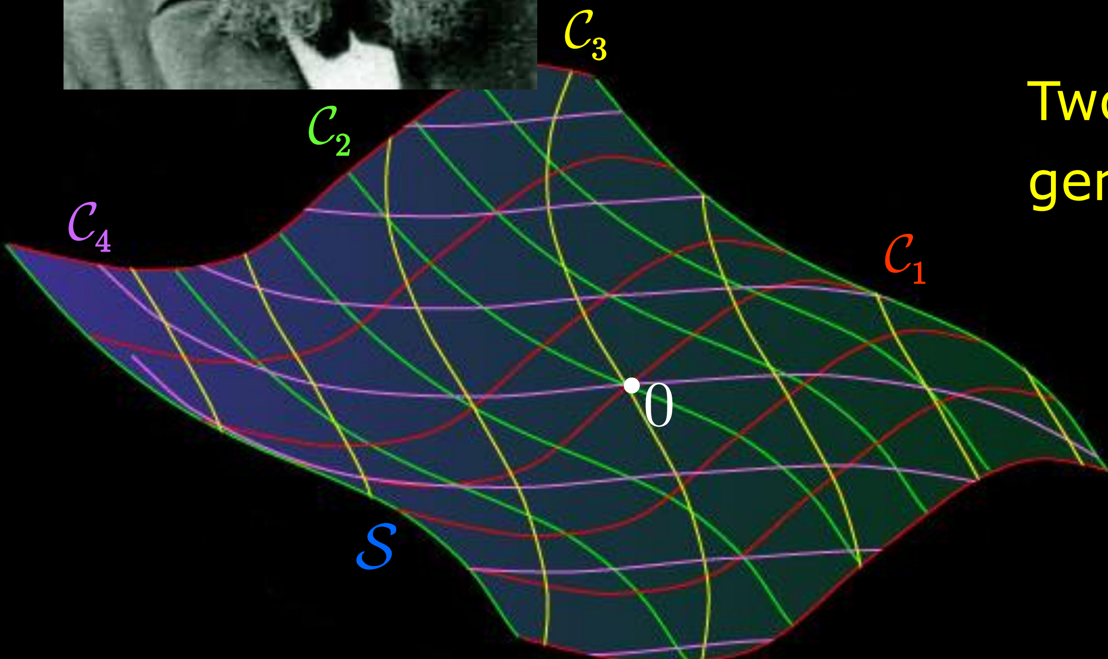


Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in 3-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$
$$= \mathcal{C}_3 + \mathcal{C}_4$$

S. Lie
1842–1899

Theorem (Lie, 1882). Consider any double translation surface in $\mathbb{C}^r$, $r \geq 3$. Then $r = 3$ and there is an algebraic curve $\mathcal{C}$ of degree 4 in the plane at infinity, such that all tangent lines to $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_4$ all pass through $\mathcal{C}$.



Two curves $\mathcal{C}_1$, $\mathcal{C}_2$ in 3-space generate surface

$$\mathcal{S} = \mathcal{C}_1 + \mathcal{C}_2$$
$$= \mathcal{C}_3 + \mathcal{C}_4$$

S. Lie
1842–1899

Theorem (Lie, 1882). Consider any double translation surface in $\mathbb{C}^r$, $r \geq 3$. Then $r = 3$ and there is an algebraic curve $\mathcal{C}$ of degree 4 in the plane at infinity, such that all tangent lines to $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_4$ all pass through $\mathcal{C}$.

Conversely, *every* algebraic curve $\mathcal{C}$ of degree 4 and algebraic genus 3 in the plane at infinity determines a double translation surface $\mathcal{S}$ in this way.

Chern called this result a *'true tour de force'*.

S. Lie
1842–1899

Lie was not thrilled.

H. Poincaré
1854–1912

Poincaré published sequels (1895, 1901) to Lie's paper, observing the connection to Abel's Theorem.

J. Little
1956–

Little's dissertation, under B. Saint-Donat, and several subsequent papers, concern webs of maximal rank.

In particular he proved an analogue (1984) over algebraically closed fields of positive characteristic.

For k-webs over $F(X,Y)$ or $F((X,Y))$, we have

$$\dim \mathcal{V}_0 \leq \tfrac{1}{2}(k\text{-}1)(k\text{-}2).$$

Equality holds iff the web is ‘cyclic’.

We want versions of this result over *finite* fields.
Here are some results for k=3,4:

Theorem (M. 1991). For a 3-net of prime order p, we have dim $\mathcal{V}_0 \leq 1$. Equality holds iff the net is cyclic.

Original proof (1991) used loop theory.

More recent proof (M. 2005) uses exponential sums; cf. Gluck's 1990 proof that a transitive affine plane of prime order is Desarguesian.

Theorem (M. 2005). For a 4-net of prime order p, we have

(a) The number of cyclic 3-subnets is 0, 1, 3 or 4.

(b) There are 4 cyclic 3-subnets iff the net is Desarguesian.

(c) If there is *at least one* cyclic subnet, then $\dim \mathcal{V}_0 \leq 3$, and equality holds iff the net is cyclic.

The proof uses exponential sums.

Part (a) is best possible.

Theorem (M. 2005). For a 4-net of prime order p, we have

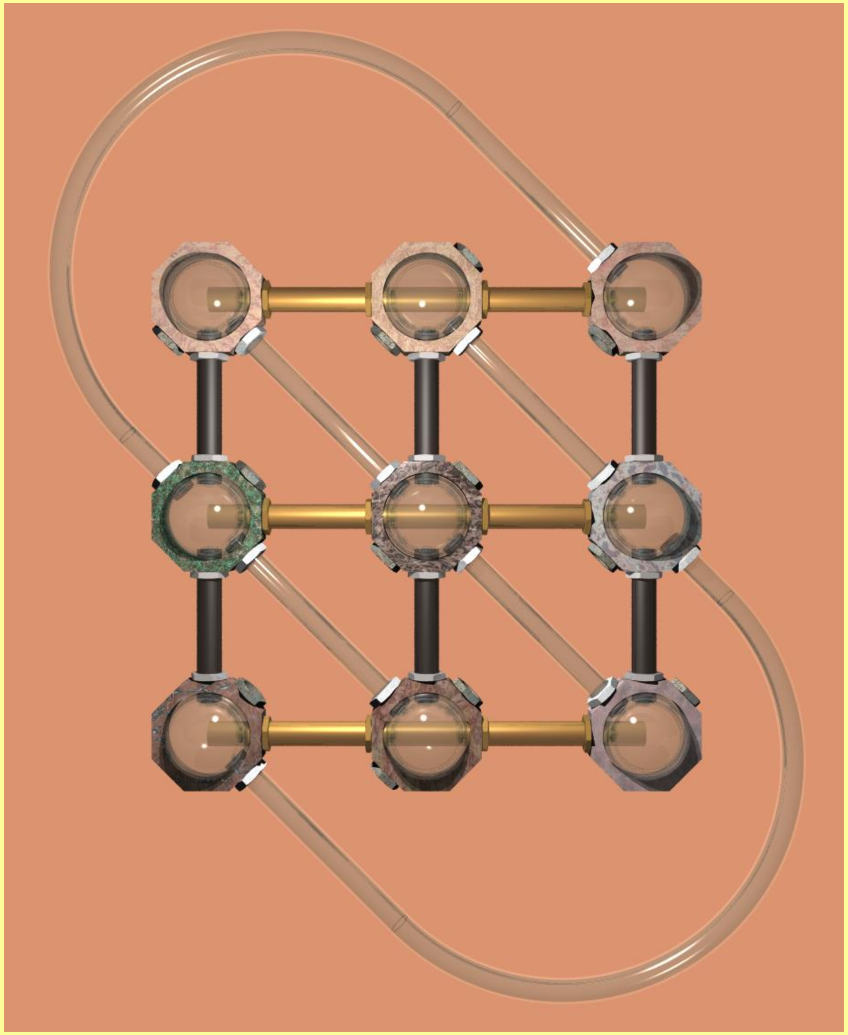
(a) The number of cyclic 3-subnets is 0, 1, 3 or 4.

(b) There are 4 cyclic 3-subnets iff the net is Desarguesian.

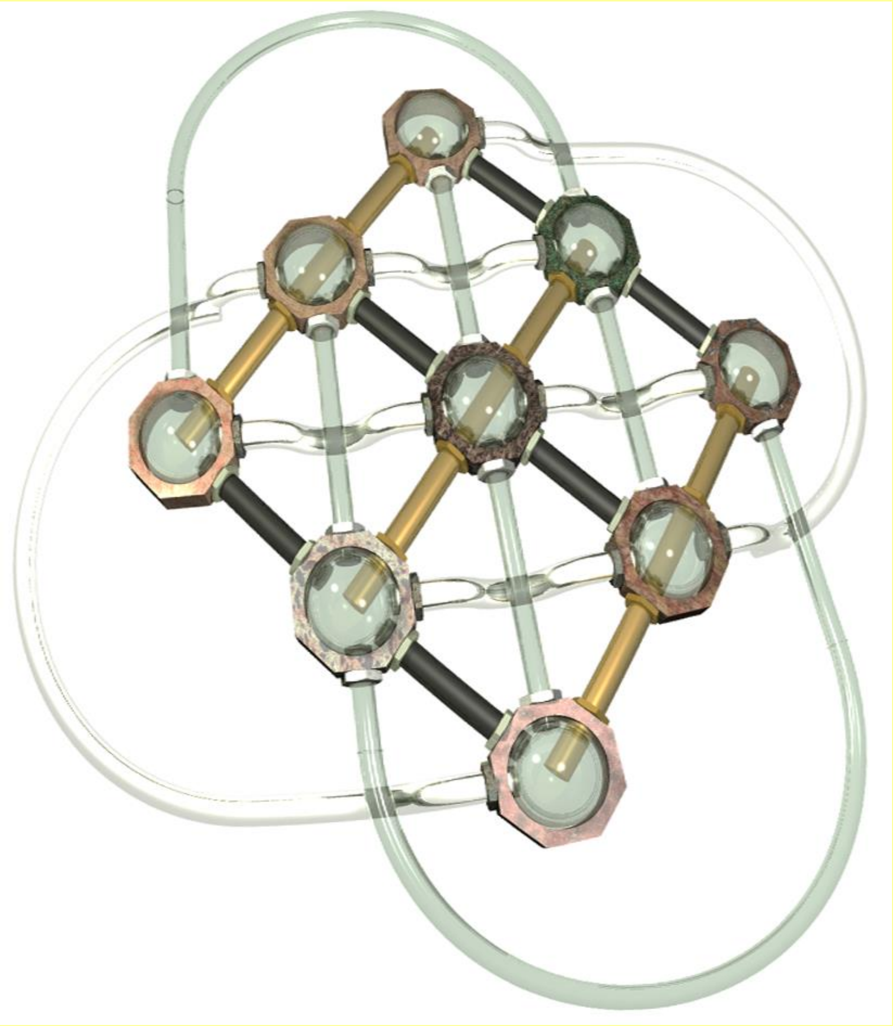
(c) If there is *at least one* cyclic subnet, then $\dim \mathcal{V}_0 \leq 3$, and equality holds iff the net is cyclic.

The proof uses exponential sums.

The same techniques can be applied in the study of MUB's (e.g. to show that MUB's in $\mathbb{C}^n$, $n \leq 5$, are unique).



3-net
of order 3



4-net
(Affine Plane)
of order 3

Thank You!

Questions?