# Good Packings

Eric Moorhouse
MUN and University of Wyoming

# Ovoids from Number Theory

Let $p \equiv 1 \mod 4$ be prime, and let $\mathcal{O}_p$ be the set of integer vectors $(x_1, \ldots, x_6)$ such that

$$x_1 \equiv x_2 \equiv \cdots \equiv x_6 \equiv 1 \mod 4;$$
$$x_1^2 + x_2^2 + \cdots + x_6^2 = 6p.$$

Then $|\mathcal{O}_p| = p^2 + 1$.

## **Example:** $p = 5$

Solve

$$x_1 \equiv x_2 \equiv \cdots \equiv x_6 \equiv 1 \mod 4;$$
$$x_1^2 + x_2^2 + \cdots + x_6^2 = 6\cdot 5 = 30.$$

Solutions:

$$\mathcal{O}_5 = \{(5,1,1,1,1,1)^*, \qquad (6 \text{ such})$$
$$(-3,-3,-3,1,1,1)^*\} \qquad (20 \text{ such})$$

Total $\qquad |\mathcal{O}_5| = 26 = 5^2 + 1$

* denotes 'all $6! = 720$ permutations thereof'

## **Example:** $p = 13$

Solve

$$x_1 \equiv x_2 \equiv \cdots \equiv x_6 \equiv 1 \mod 4;$$
$$x_1^2 + x_2^2 + \cdots + x_6^2 = 6{\cdot}13 = 78.$$

Solutions:

$$\begin{aligned} \mathcal{O}_{13} = \{&(-7,5,1,1,1,1)^*, && \text{(30 such)}\\ &(5,5,5,1,1,1)^*, && \text{(20 such)}\\ &(-7,-3,-3,-3,1,1)^*, && \text{(60 such)}\\ &(5,5,-3,-3,-3,1)^*\} && \text{(60 such)} \end{aligned}$$

Total $|\mathcal{O}_{13}| = 170 = 13^2 + 1$

---

$*$ denotes 'all $6! = 720$ permutations thereof'

## More Ovoids from Number Theory

Let $p \equiv 1 \mod 4$ be prime, and let $\mathcal{O}'_p$ be the set of integer vectors $(x_1, \ldots, x_6)$ such that

$$x_1{+}1 \equiv x_2 \equiv x_3 \equiv \cdots \equiv x_6 \mod 2;$$

$$\sum x_i \equiv 3 \mod 4;$$

$$x_1^2 + x_2^2 + \cdots + x_6^2 = p.$$

Then $|\mathcal{O}'_p| = p^2 + 1$.

## Example: $p = 5$

Solve

$$x_1 + 1 \equiv x_2 \equiv x_3 \equiv \cdots \equiv x_6 \mod 2;$$
$$\sum x_i \equiv 3 \mod 4;$$
$$x_1^2 + x_2^2 + \cdots + x_6^2 = 5.$$

Solutions:

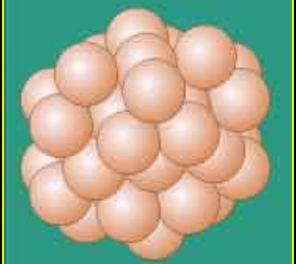
$$\mathcal{O}_5' = \{(0| \pm 1, \pm 1, \pm 1, \pm 1, \pm 1), \quad (16 \text{ such})$$
$$(1| \pm 2, 0, 0, 0, 0)\} \quad (10 \text{ such})$$

Total $|\mathcal{O}_5'| = 26 = 5^2 + 1$

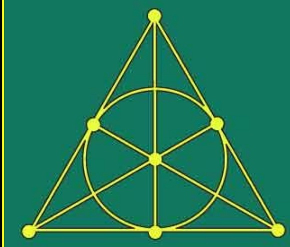
Number-theoretic ovoids

$$x_1^2+x_2^2+\ldots+x_6^2 = 6p$$

Sphere packing in $\mathbb{R}^8$ → … → Number-theoretic ovoids → … → New projective planes



$$x_1^2+x_2^2+\ldots+x_6^2 = 6p$$



*At each step we have an optimal packing.*

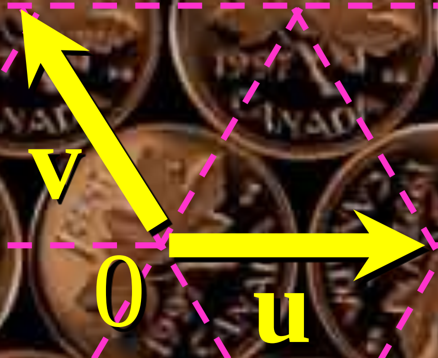

1 CENT
1997
CANADA

# What is the densest possible packing of (nonoverlapping) uniform disks in the plane?


1 CENT
1997
CANADA

# The densest plane packing is the hexagonal lattice packing: centres of the disks are points of the $A_2$ (hexagonal) lattice

$$L = \{a\mathbf{u} + b\mathbf{v} : a, b \in \mathbb{Z}\}$$



A *lattice* in $\mathbb{R}^n$ is a subset

$$L = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \; : \; a_1, a_2, \ldots, a_n \in \mathbb{Z}\}$$

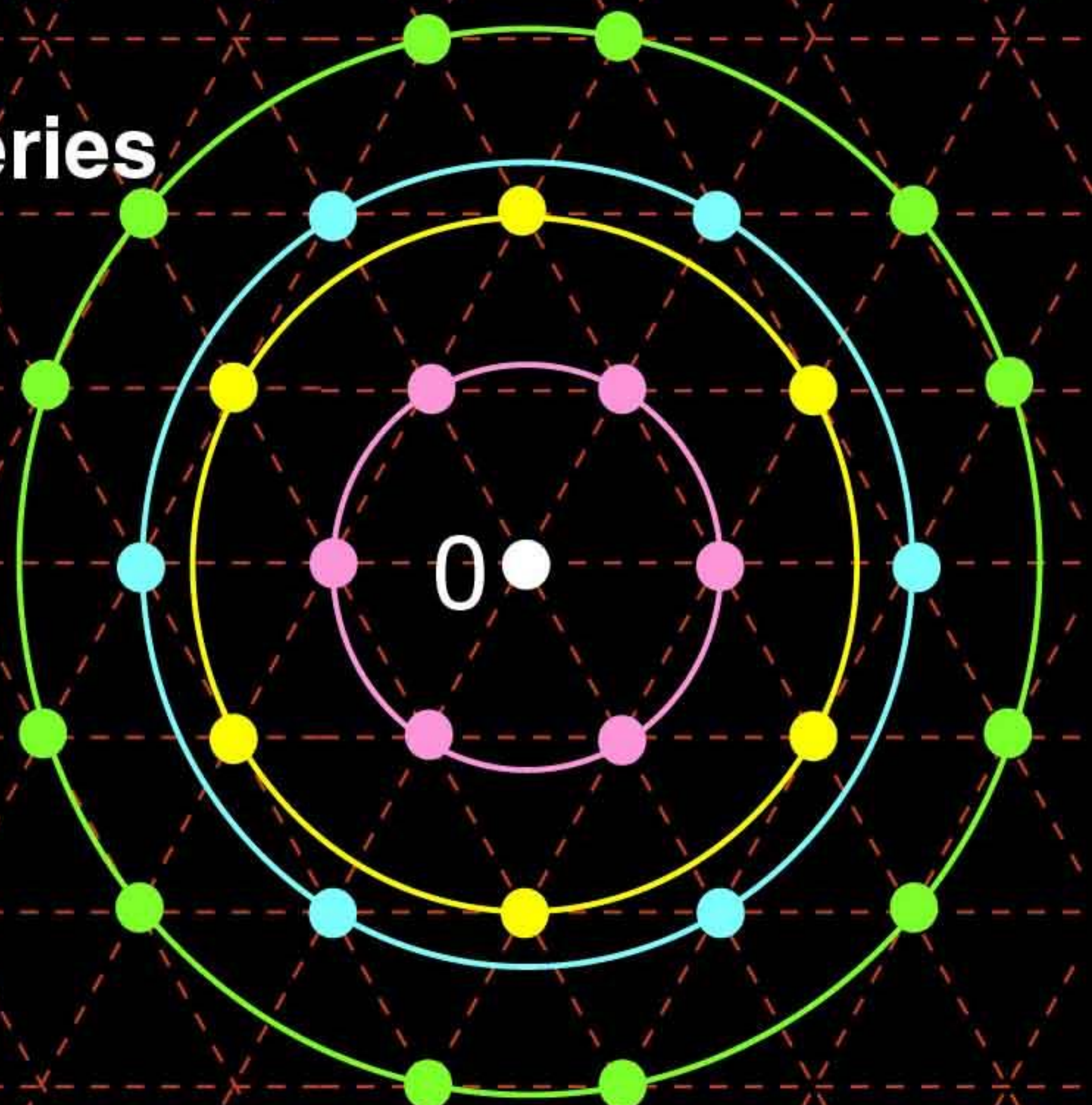
where $v_1, v_2, \ldots, v_n$ is a basis for $\mathbb{R}^n$ over $\mathbb{R}$.

The *theta series of* $L$ is

$$\Theta_L(z) = \sum_{v \in L} q^{\|v\|^2} \quad \text{where} \quad q = e^{\pi i z},$$

convergent for $|q| < 1$, i.e. $Re(z) > 0$.

E.g. the theta series of the $A_2$ lattice

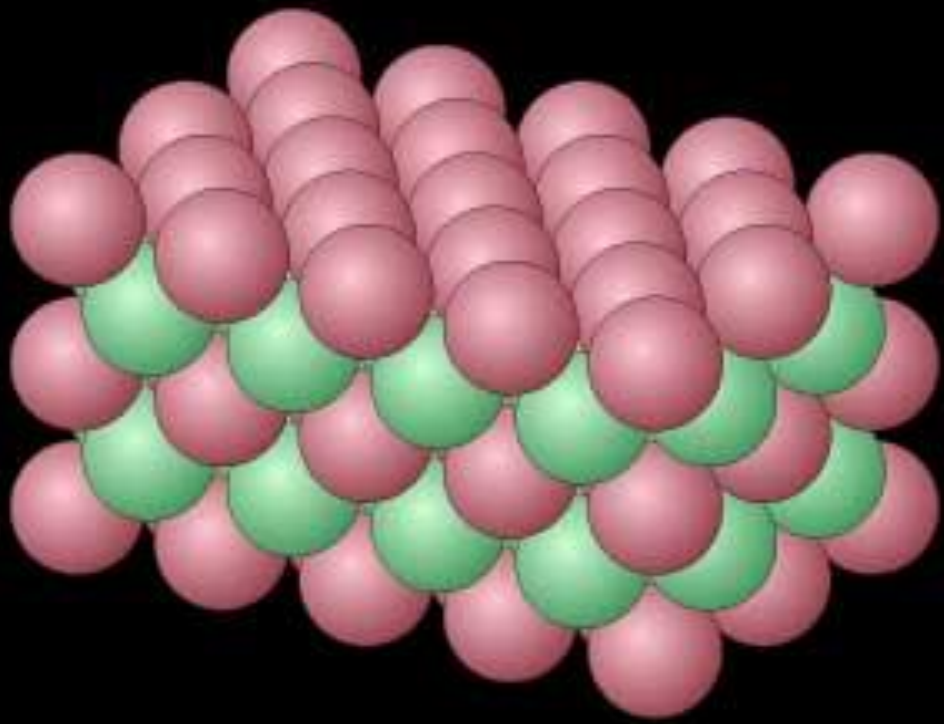



$$\Theta(z) = 1 + 6q + 6q^3 + 6q^4 + 12q^7 + \cdots$$

# Face Centred Cubic ($A_3$ lattice) Packing

**Theorem**
**(Hales 1997)**

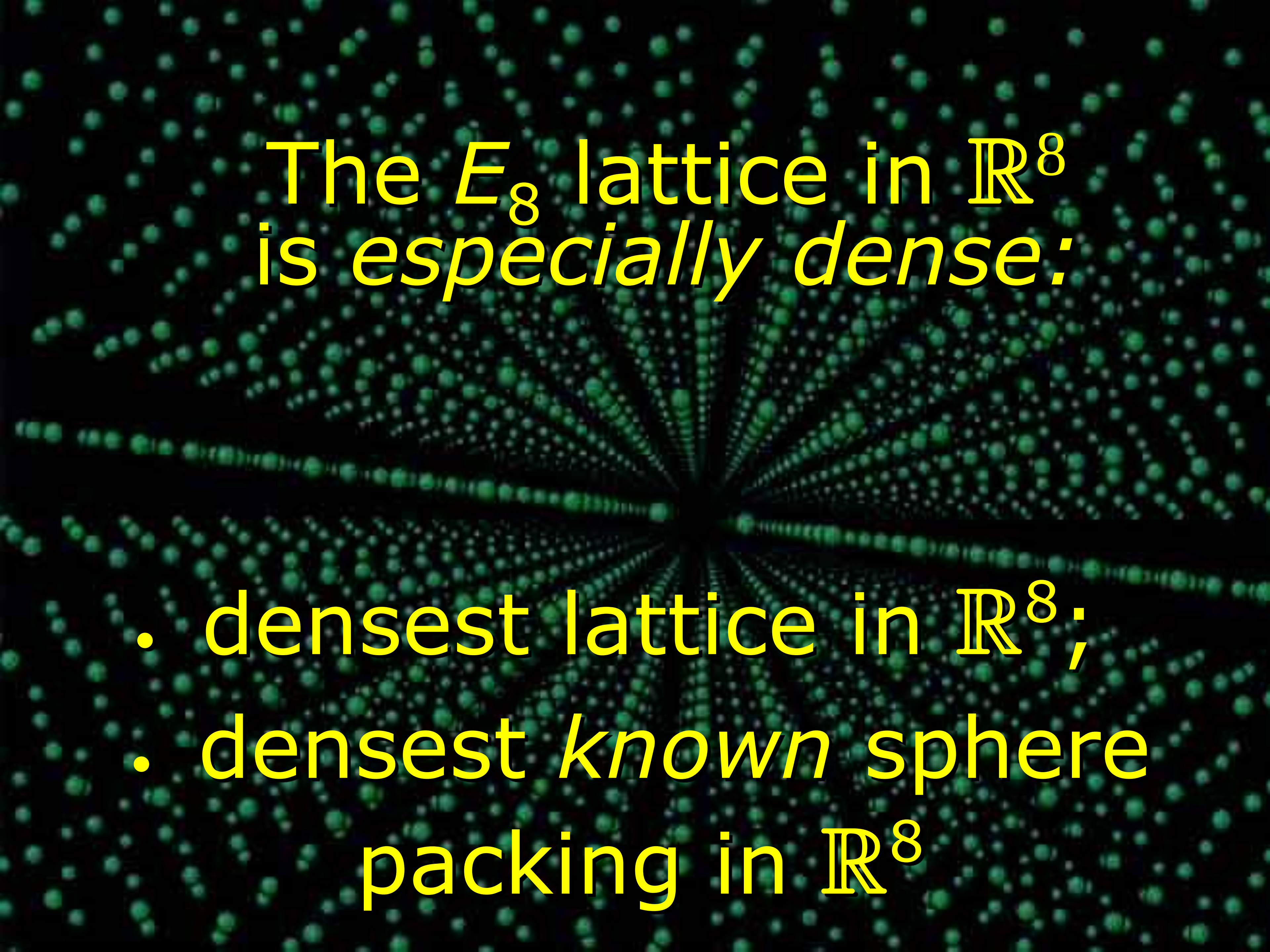
*This is the densest sphere packing in* $\mathbb{R}^3$.



oblique view

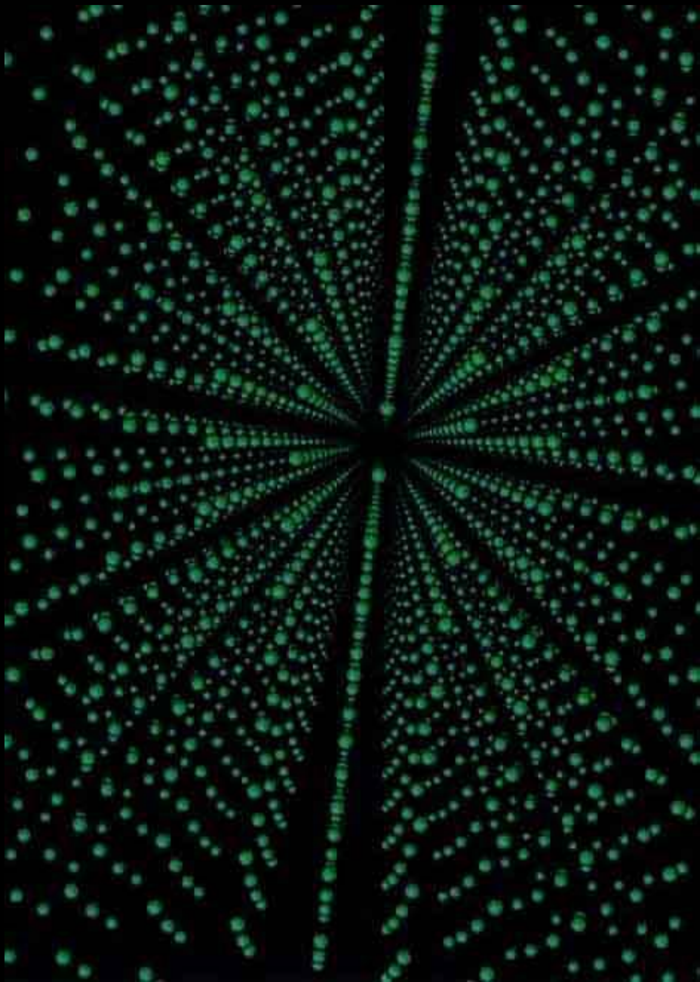
# Theta series of the $A_3$ lattice

$$\Theta(z) = 1 + 12q^2 + 6q^4 + 24q^6 + \cdots$$


The $E_8$ lattice in $\mathbb{R}^8$
is *especially dense:*
• densest lattice in $\mathbb{R}^8$;
• densest *known* sphere packing in $\mathbb{R}^8$

Theta series of the $E_8$ lattice in $\mathbb{R}^8$

$$\Theta(z) = 1 + 240q^2 + 2160q^4 + 6720q^6 + \cdots$$
$$= 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^{2m}$$



where

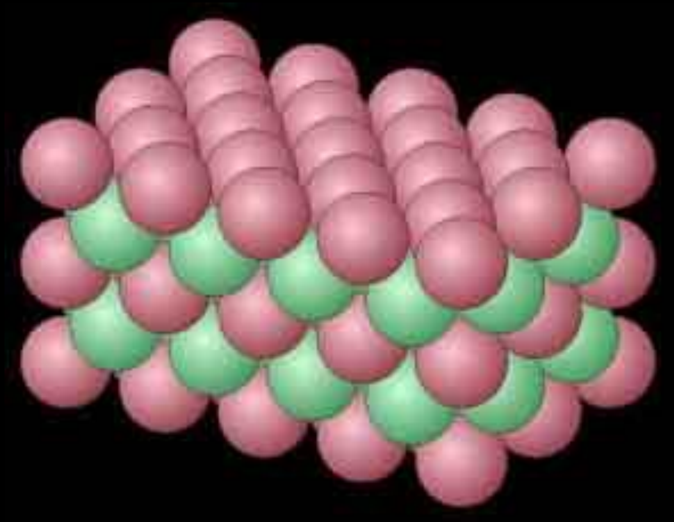
$$\sigma_3(m) = \sum_{d|m} d^3$$

e.g. $\sigma_3(1) = 1^3 = 1$;

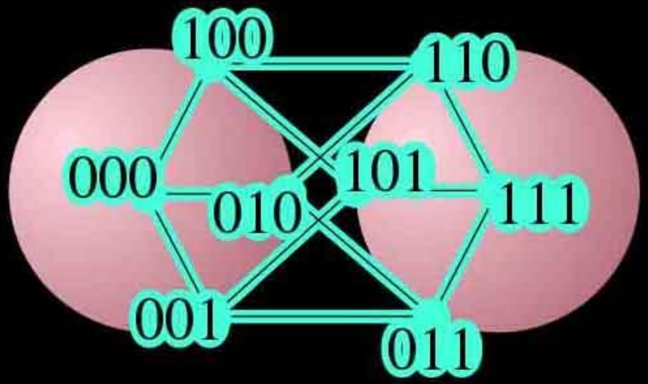
$\sigma_3(p) = p^3 + 1$ for $p$ prime

Packings in Euclidean space

Packings in discrete spaces



sphere packings




e.g. theory of error-correcting codes

# *Finite fields*

For every prime $p$,

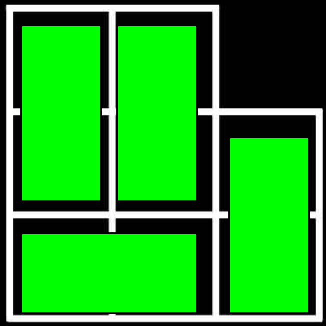
$$\mathbb{F}_p = \{0, 1, 2, \ldots, p\text{-}1\}$$

is the field of integers mod $p$.

For each $p^k$ there is a field $\mathbb{F}_{p^k}$ of order $|\mathbb{F}_{p^k}| = p^k$.
This is *not* the integers mod $p^k$ unless $k=1$.

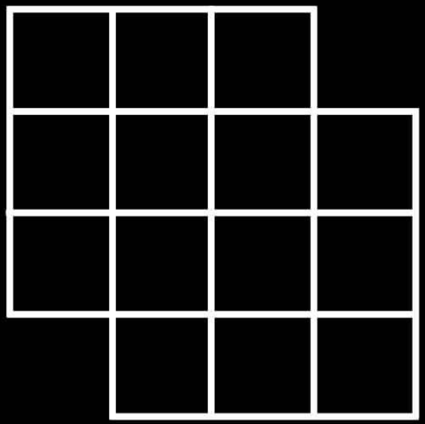
Most algebraic properties of $\mathbb{F}_{p^k}$, and geometric properties of the spaces they coordinatise, hold uniformly for all $p^1$, $p^2$, $p^3$, … (But we will see an exception where $p^1$ is special.)

## Sample Packing Problem



Tile this figure
using $2 \times 1$ dominoes.

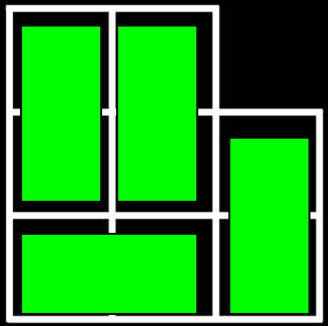
One, of several, solutions.
Such a complete tiling we'll call a *spread*.



This figure
has *no spread* of dominoes:

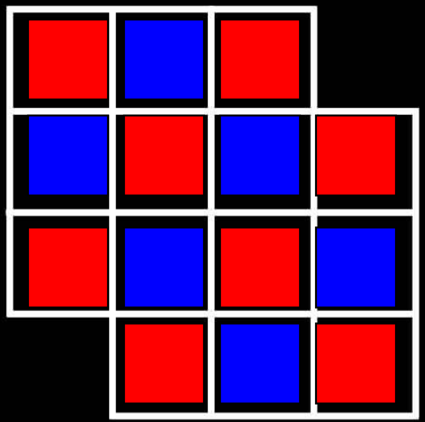
# Sample Packing Problem

Tile this figure
using $2 \times 1$ dominoes.



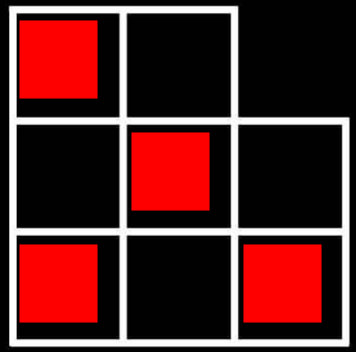
One, of several, solutions.
Such a complete tiling we'll call a *spread*.

This figure
has *no spread* of dominoes:



# The Dual Packing Problem

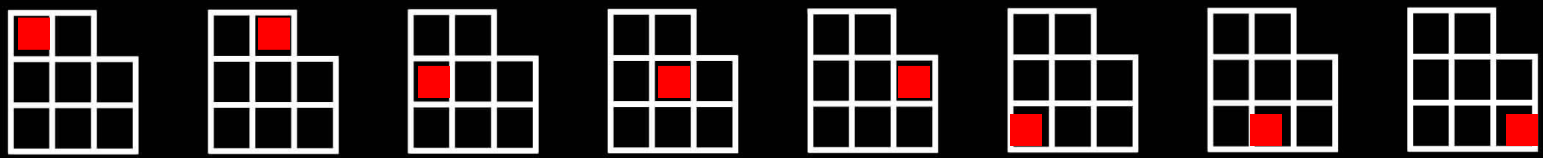
Find a set of cells
meeting each domino
exactly once.

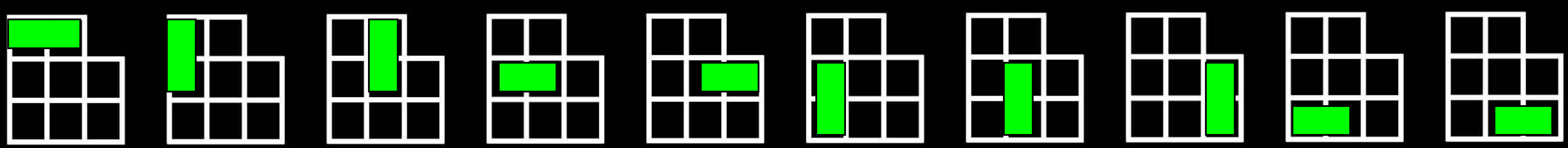


One of two solutions.
Such a set of cells we'll call an *ovoid*.

Why is this problem dual to the previous one?

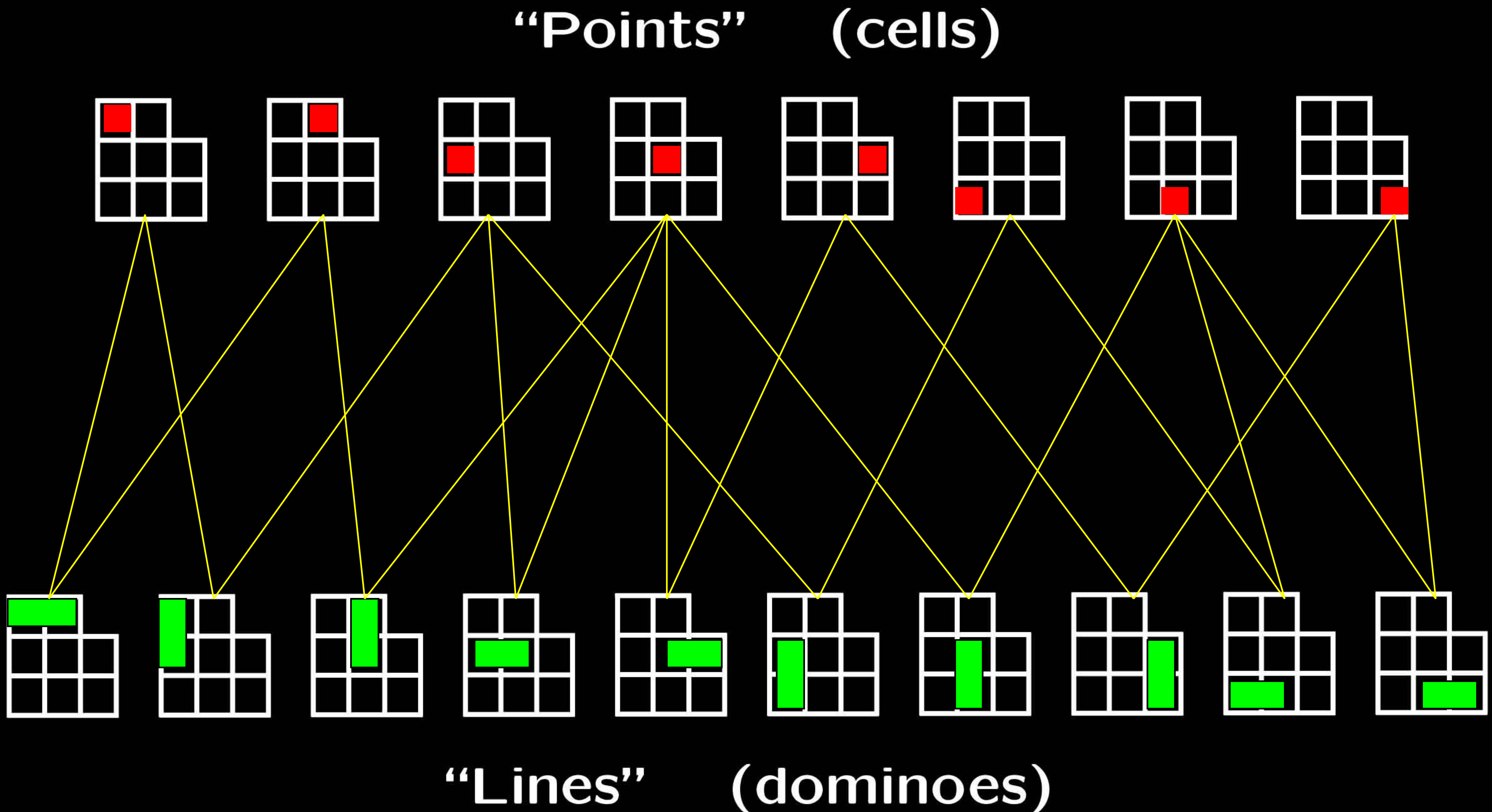
“Points” (cells)



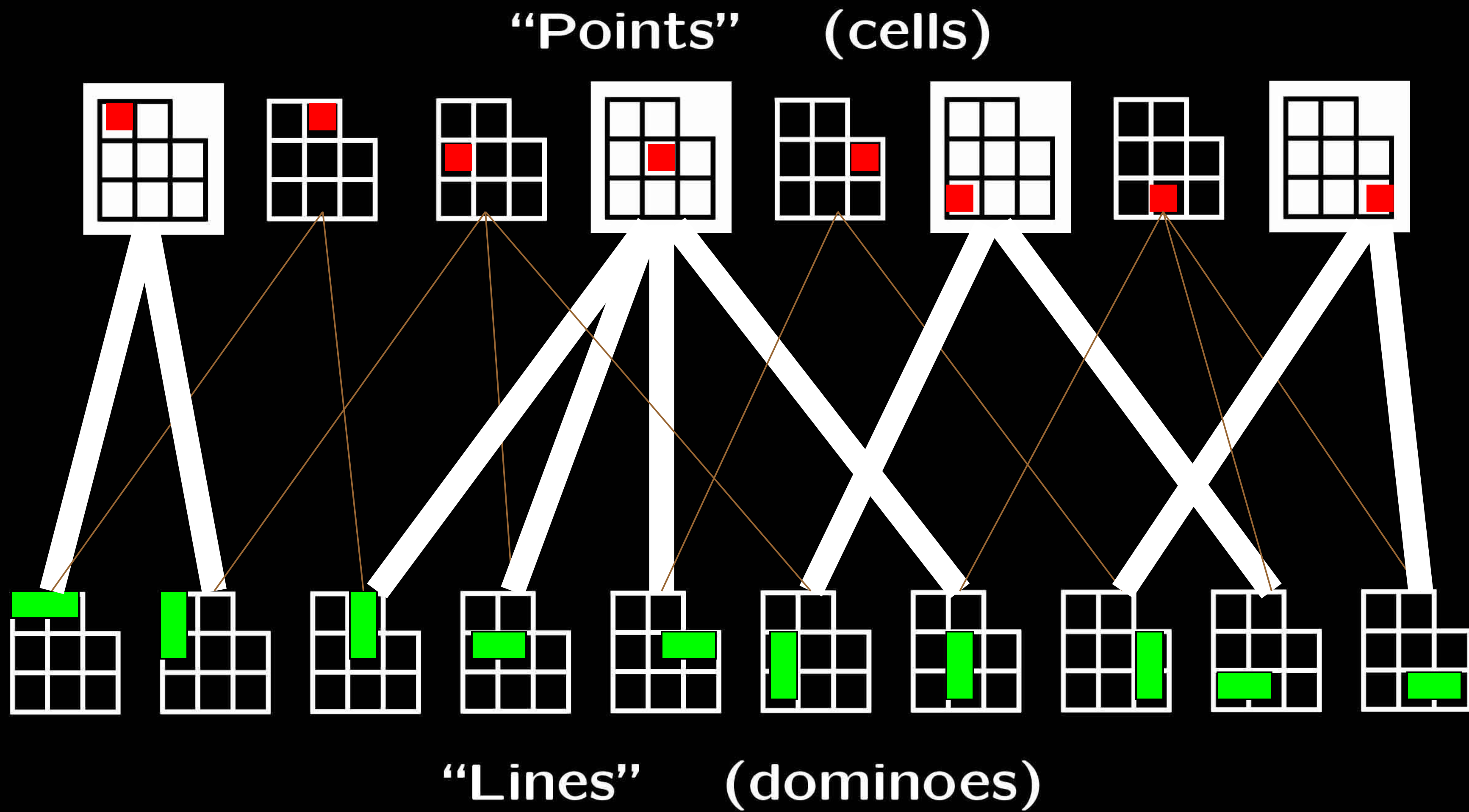


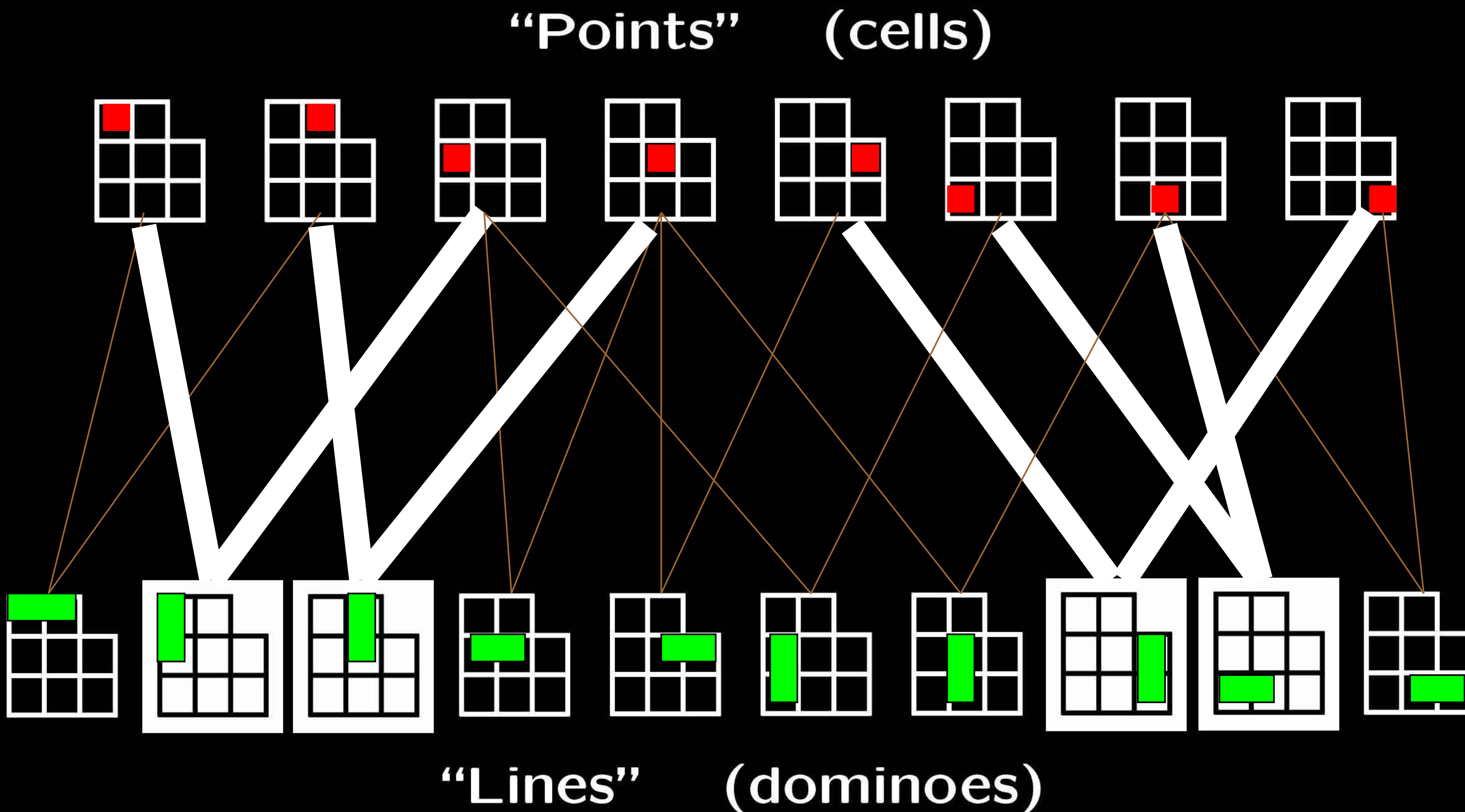
“Lines” (dominoes)

# *bipartite graph:*



# Ovoid






**Spread**

## Definitions

Given:

- a set $\mathcal{P}$ of "points", and
- a collection $\mathcal{B}$ of "blocks" or "lines" (certain subsets of $\mathcal{P}$)

An *ovoid* is a point set $\mathcal{O} \subseteq \mathcal{P}$ such that each block contains exactly one point of $\mathcal{O}$.

Dually,

A *spread* is a set of blocks $\Sigma \subseteq \mathcal{B}$ which partitions the point set $\mathcal{P}$.

*Spread of 3-space $P^3\mathbb{F}$:*

a set of lines partitioning the points

E.g. the simplest spread of $P^3\mathbb{R}$:

Take all complex 1-dimensional subspaces of $\mathbb{C}^2=\mathbb{R}^4$.

These partition the points of $P^3\mathbb{R}$ into projective lines (real 2-subspaces).

## *Spread of 3-space $P^3\mathbb{F}_p$:*

a set of lines partitioning the points

no. of lines in spread

no. of points per line

no. of points in 3-space $= (p^2+1)(p+1)$

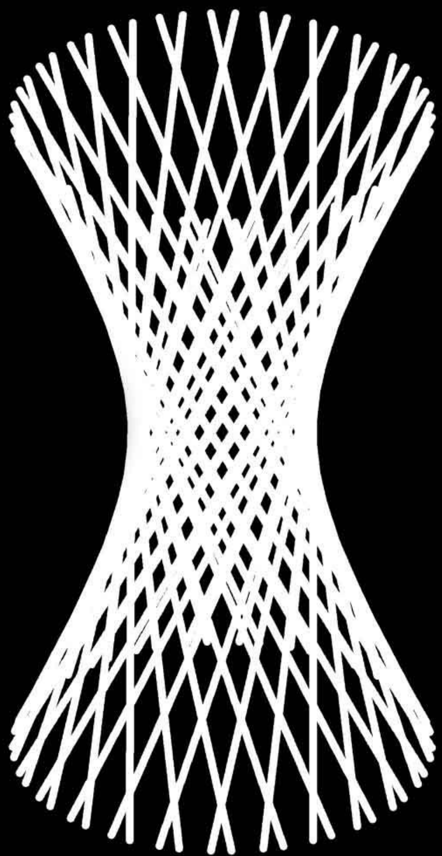
# Ovoids and Spreads of Quadrics

Consider the quadric

$$\mathcal{Q}: \quad x_1^2 + x_2^2 + \cdots + x_n^2 - y_1^2 - y_2^2 = 0$$

in $\mathbb{R}^{n+2}$, $n \geq 2$. Define

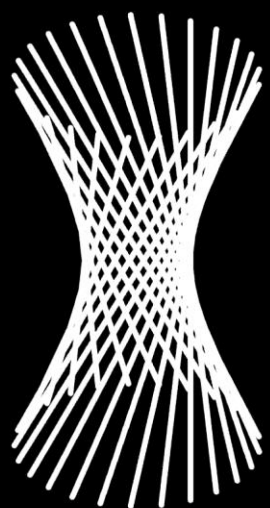
$\mathcal{P} = \{$1-dimensional subspaces in $\mathcal{Q}\}$
$\mathcal{B} = \{$2-dimensional subspaces in $\mathcal{Q}\}$



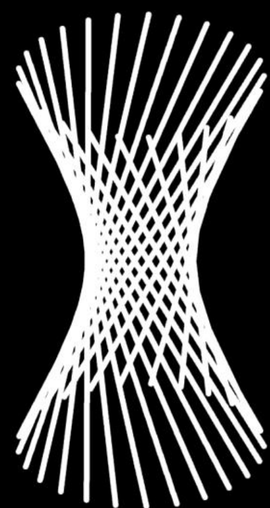
Shown: case $n = 2$

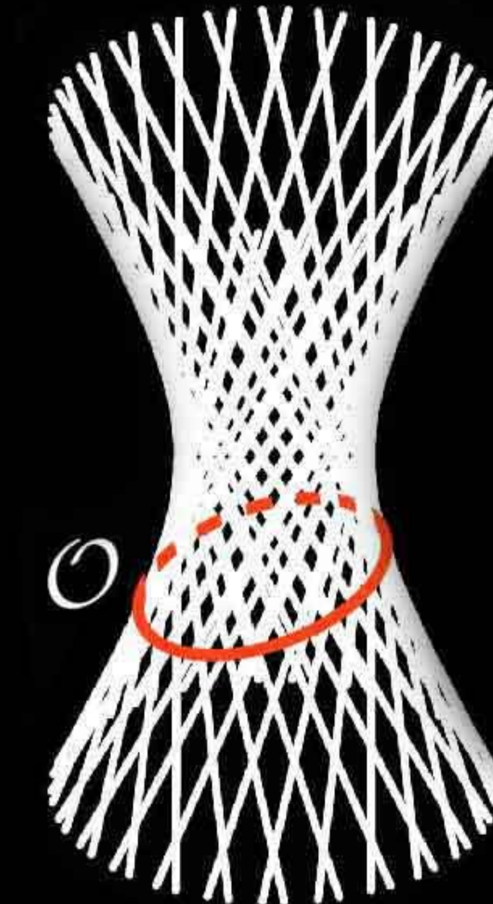
This quadric has two spreads:

$\Sigma_1$ :



$\Sigma_2$ :






and *many* ovoids, e.g.

$$\mathcal{O} = \{(x_1, \ldots, x_n, 1, 0) : x_1^2 + x_2^2 + \cdots + x_n^2 = 1\}$$

All quadrics in $P^n\mathbb{R}$ have ovoids
but not all have spreads.

For finite $\mathbb{F}$: existence of ovoids
and spreads in $P^n\mathbb{F}$ quadrics
depends on $n$ and $|\mathbb{F}|$.
No ovoids are known for $n > 7$.

Any ovoid or spread in
in a $P^{2n}\mathbb{F}_p$ or in $P^{2n+1}\mathbb{F}_p$ quadric
has size $p^n+1$.

All quadrics in $P^n\mathbb{R}$ have ovoids but not all have spreads.

For finite $\mathbb{F}$: existence of ovoids and spreads in $P^n\mathbb{F}$ quadrics depends on $n$ and $|\mathbb{F}|$.
No ovoids are known for $n > 7$.

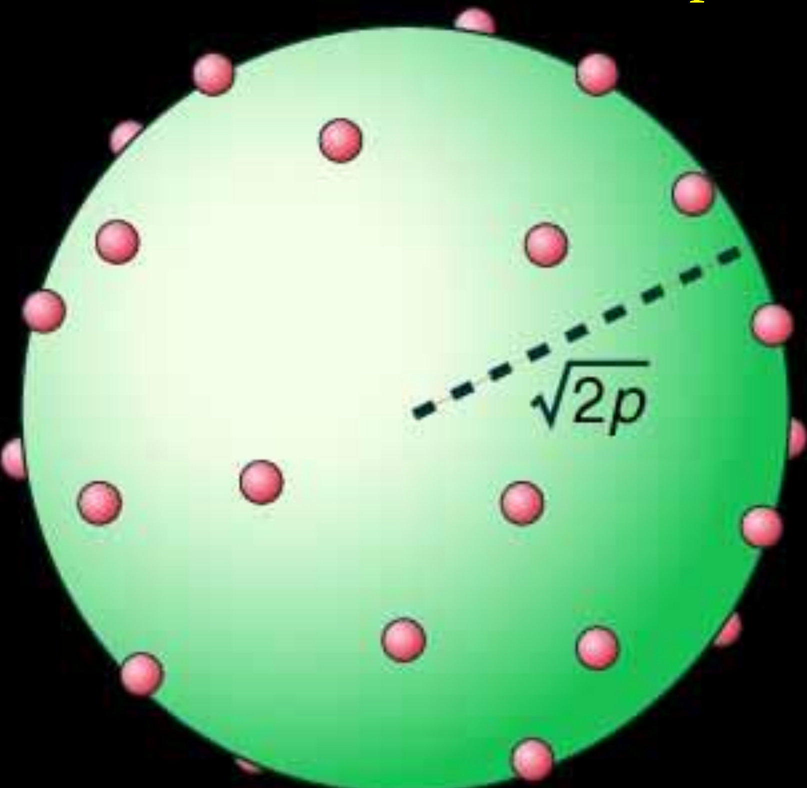
Ovoids do not exist in

- $P^{2n}\mathbb{F}$, $n \geq 4$ (Gunawardena and M., 1997);
- $P^9\mathbb{F}$, $|\mathbb{F}|=2^k$ or $3^k$ (Blokhuis and M., 1995);
- $P^{11}\mathbb{F}$, $|\mathbb{F}|=2^k$, $3^k$ , $5^k$ or $7^k$ (Blokhuis and M., 1995); etc.

Some ovoids of quadrics in $P^7\mathbb{F}_p$ discovered by John H. Conway (1988)

# Conway's ovoids in $P^7\mathbb{F}_p$ quadrics

sphere of radius $\sqrt{2p}$ in $\mathbb{R}^8$




The $E_8$ lattice has $240\sigma_3(p) = 240(p^3+1)$ vectors of length $\sqrt{2p}$ .

Let $x \in E_8$ of length $\sqrt{2}$ (one of 240 *root vectors*).

The sublattice $\mathbb{Z}x + 2E_8$ has $p^3+1$ pairs of vectors $\pm v$.

This gives an ovoid mod $p$.

# Ovoids of $P^7\mathbb{F}_p$ quadrics

Conway (1988) construction

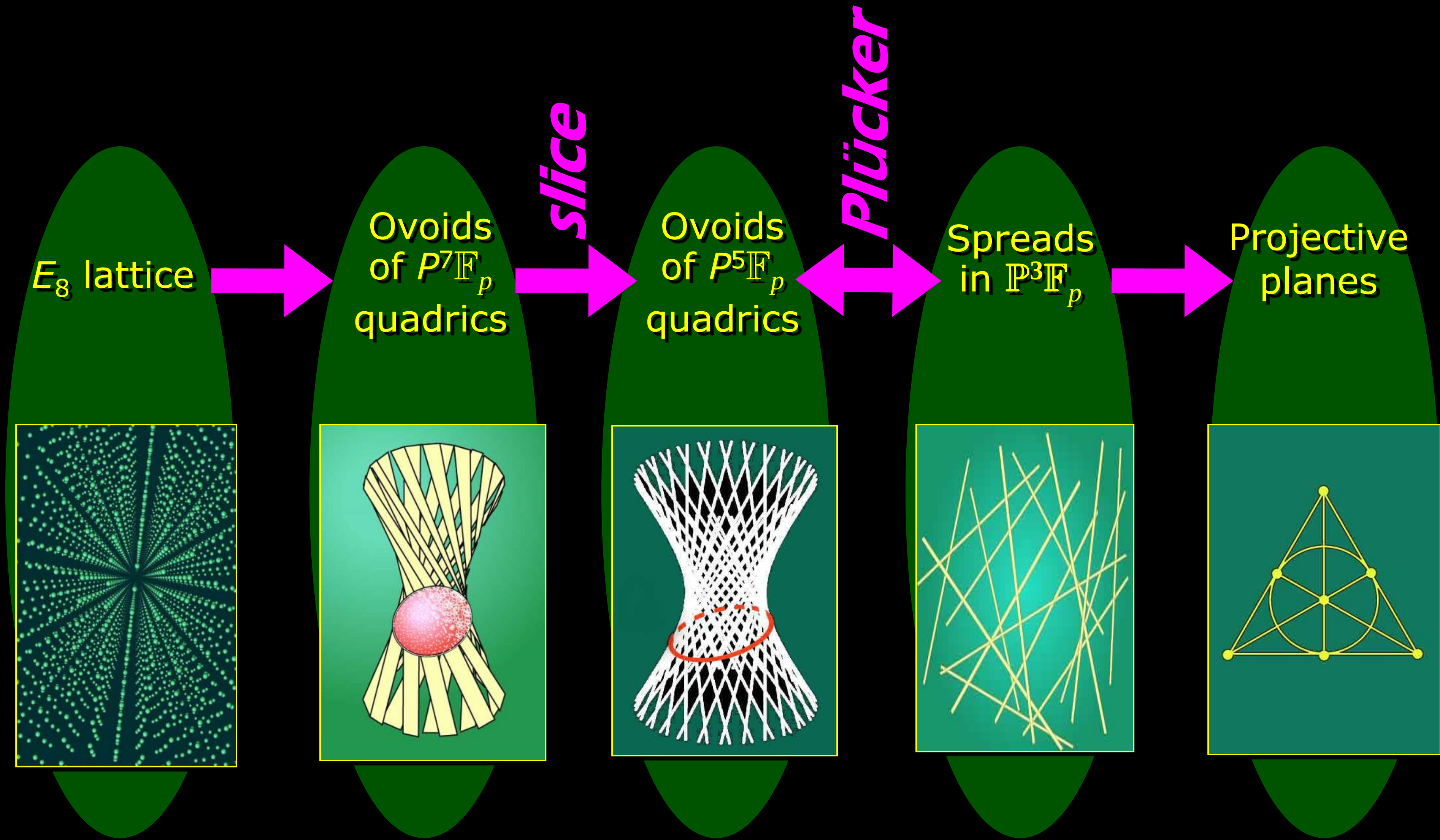
1. Shows existence of at least one ovoid for every $p$
2. Proof requires theta series of $E_8$:

$$1+240\sum_m \sigma_3(m)q^{2m}$$

Generalised construction by M. (1993, 1997)

1. Number of ovoids $\to\infty$ as $p\to\infty$
2. Proof requires theta series of $E_8 \oplus E_8$:

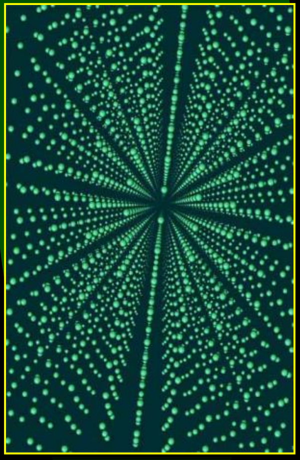
$$1+480\sum_m \sigma_7(m)q^{2m}$$



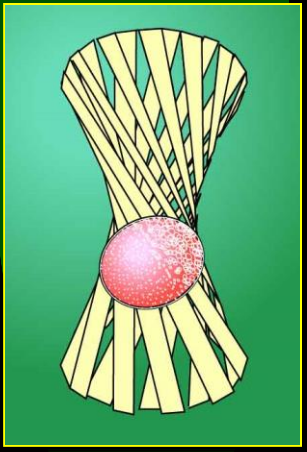
$E_8$ lattice
Ovoids of $P^7\mathbb{F}_p$ quadrics
slice
Ovoids of $P^5\mathbb{F}_p$ quadrics
Plücker
Spreads in $\mathbb{P}^3\mathbb{F}_p$
Projective planes

Conway, Kleidman, Wilson (1988); M. (1993, 1997)

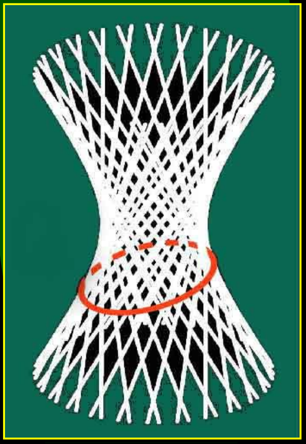
$E_8$ lattice



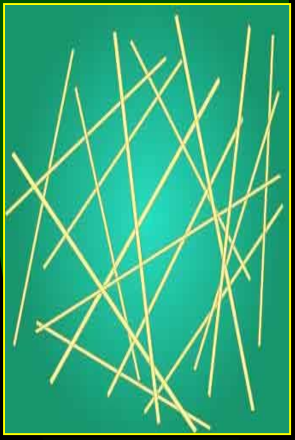
Ovoids of $P^7\mathbb{F}_p$ quadrics



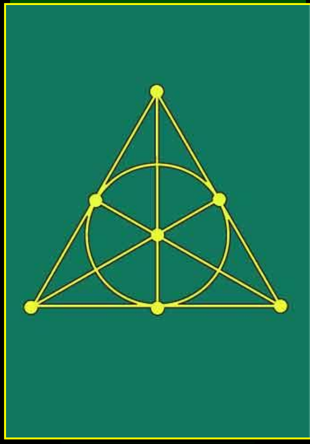
Ovoids of $P^5\mathbb{F}_p$ quadrics



Spreads in $\mathbb{P}^3\mathbb{F}_p$



Projective planes

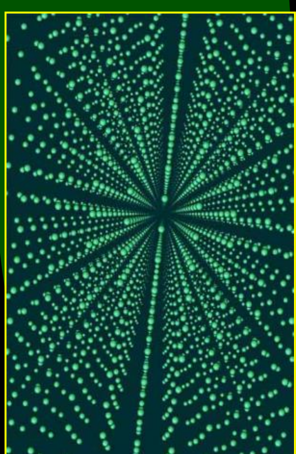


slicing

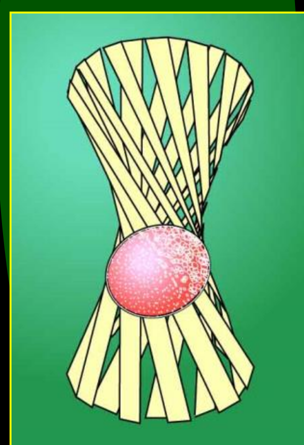
a $P^7\mathbb{F}$ ovoid

gives a $P^5\mathbb{F}$ ovoid

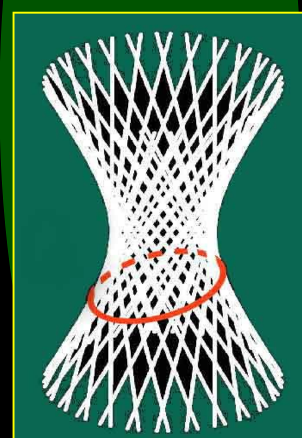
$E_8$ lattice



Ovoids of $P^7\mathbb{F}_p$ quadrics

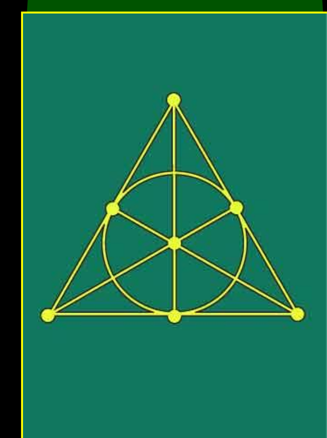


Ovoids of $P^5\mathbb{F}_p$ quadrics



Spreads in $\mathbb{P}^3\mathbb{F}_p$

Projective planes



Plücker map …

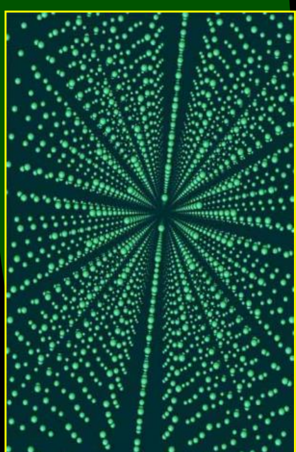
$E_8$ lattice

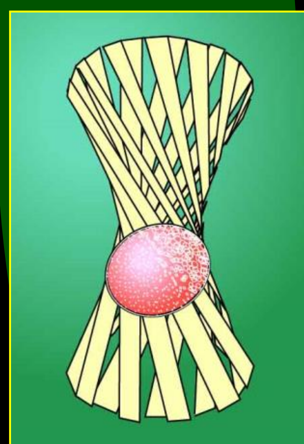
Ovoids of $P^7\mathbb{F}_p$ quadrics

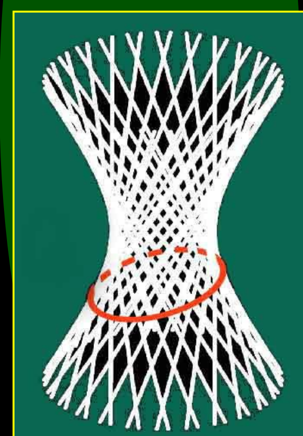
Ovoids of $P^5\mathbb{F}_p$ quadrics

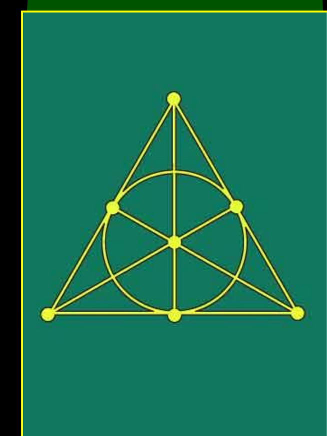
Spreads in $\mathbb{P}^3\mathbb{F}_p$

Projective planes

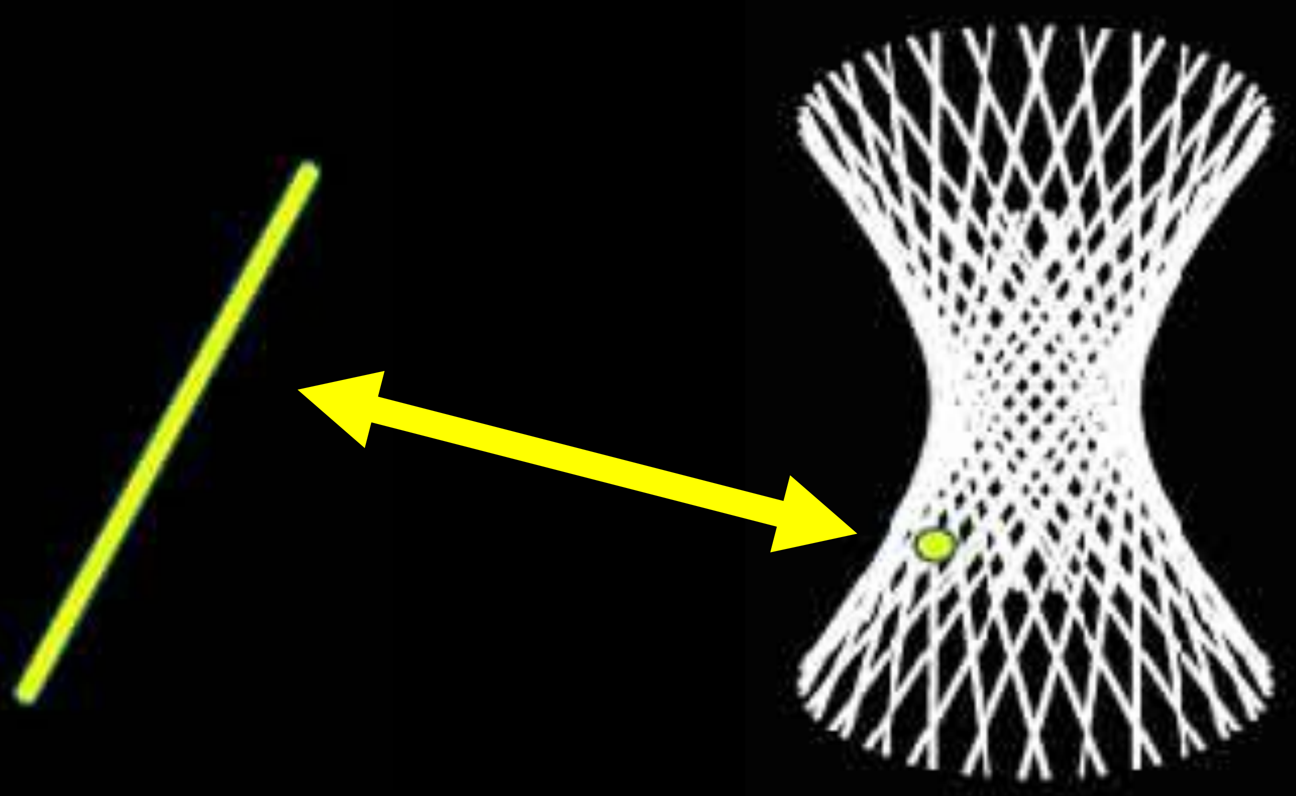








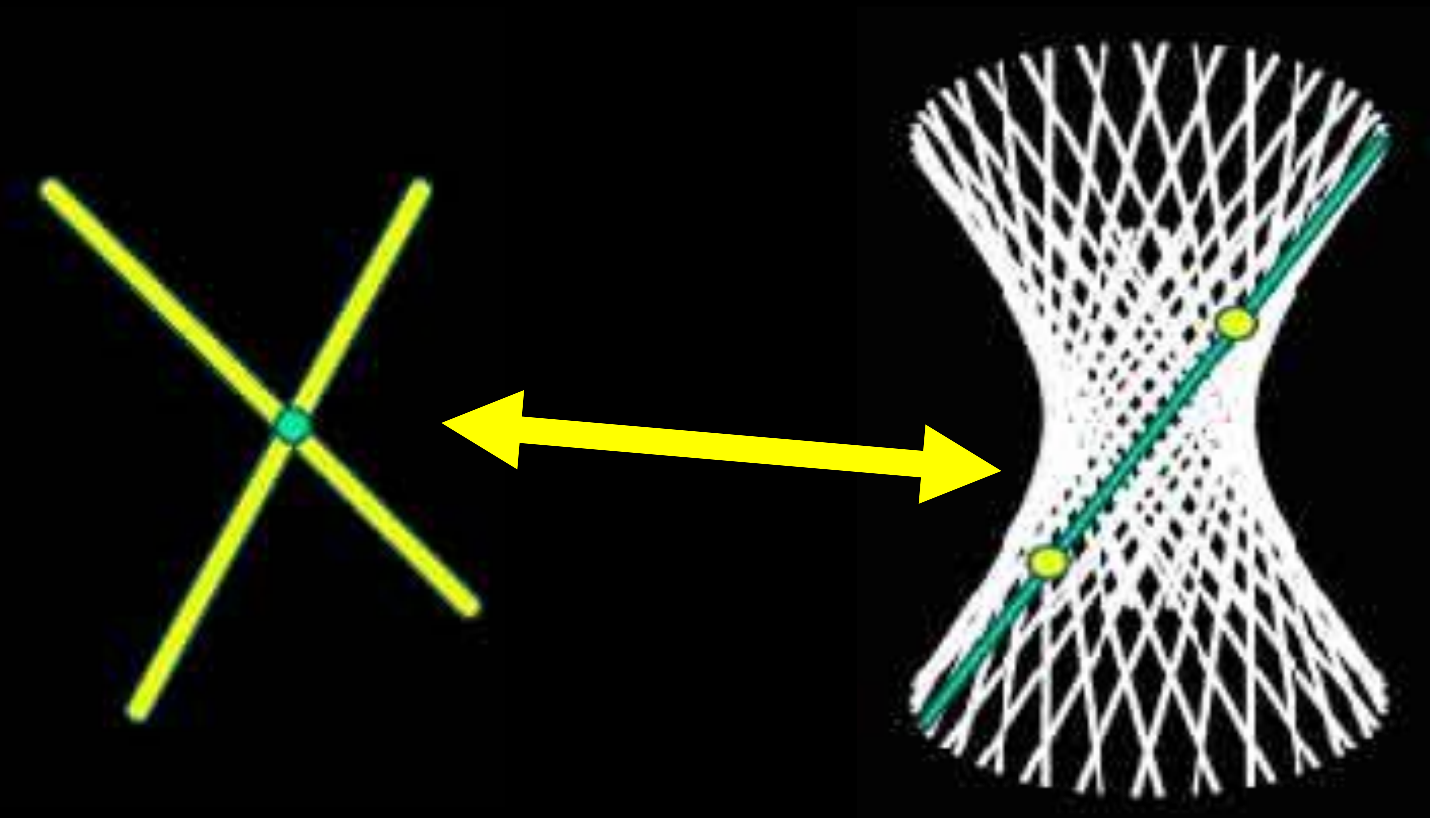
# *Plücker map*



line of $P^3\mathbb{F}_p$

point of $P^5\mathbb{F}_p$ quadric

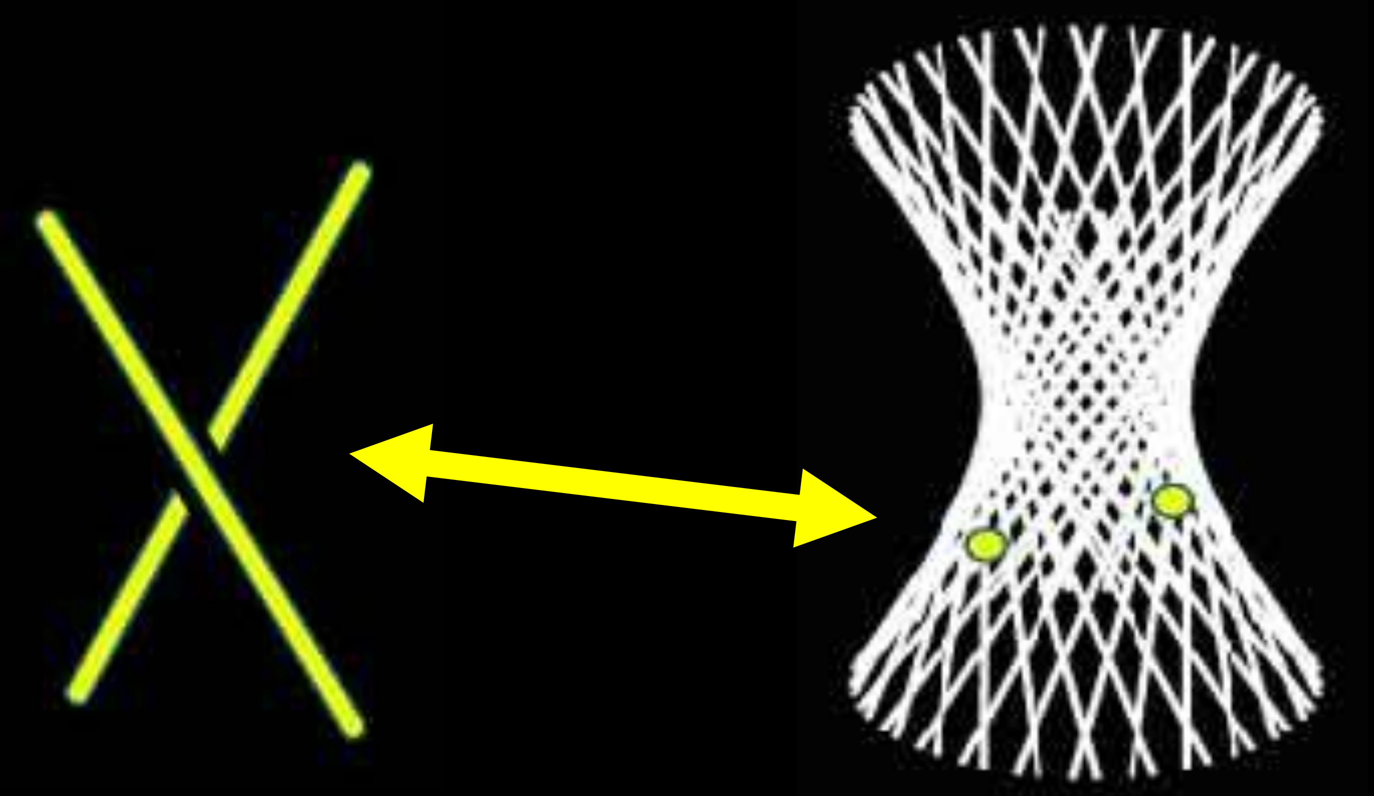
# *Plücker map*



pair of intersecting lines of $P^3\mathbb{F}_p$

pair of points of $P^5\mathbb{F}_p$ quadric on a line of the quadric

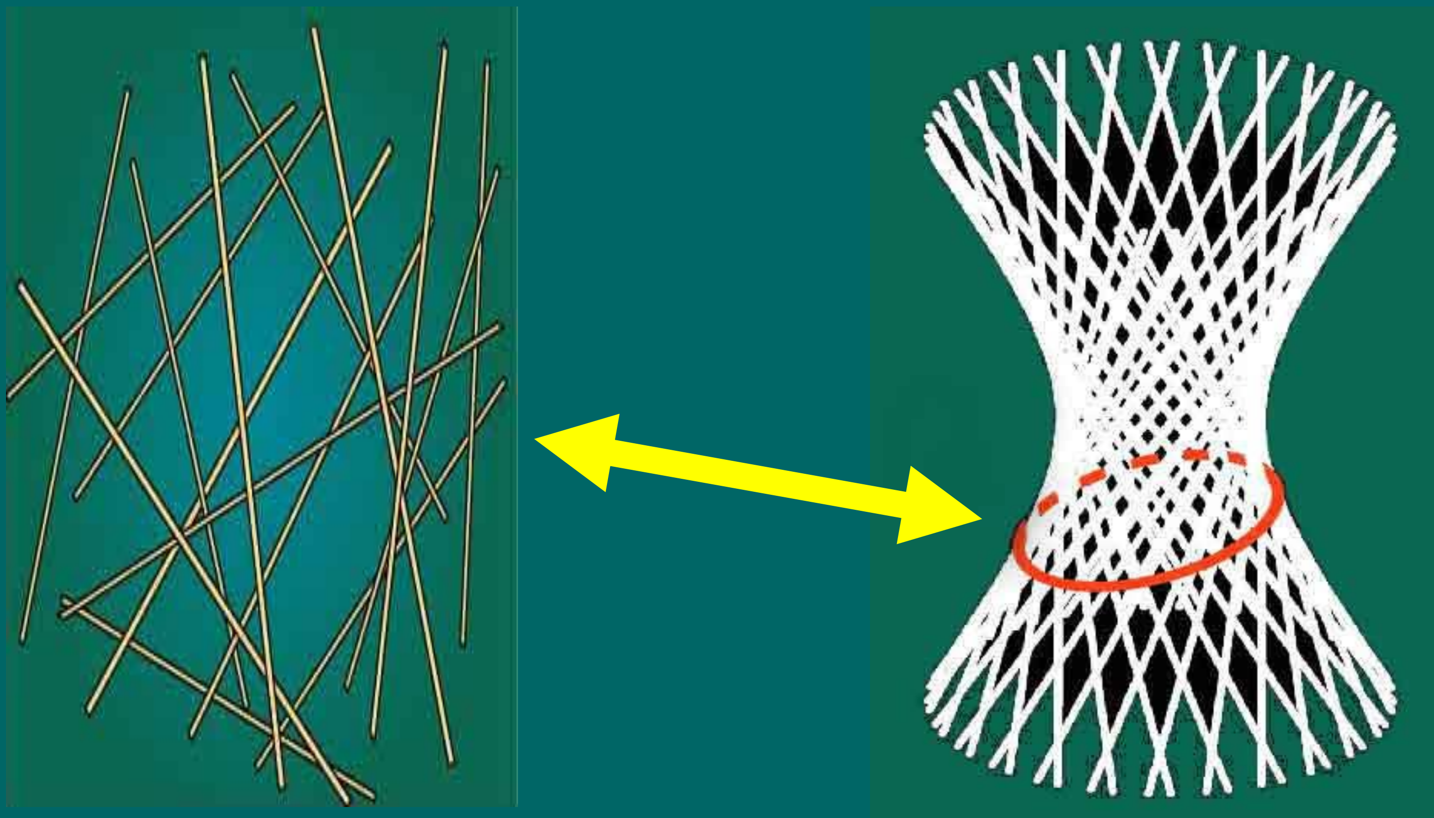
# *Plücker map*



pair of skew
lines of $P^3\mathbb{F}_p$

pair of points
of $P^5\mathbb{F}_p$ quadric
not on a line of the quadric

# *Plücker map*



spread of $P^3\mathbb{F}_p$

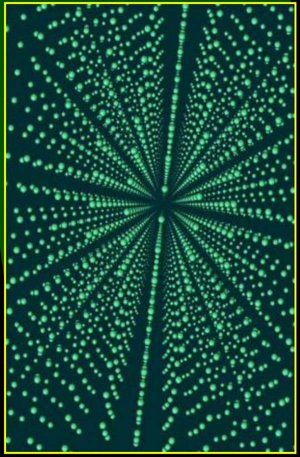
$p^2+1$ mutually skew lines

ovoid of $P^5\mathbb{F}_p$ quadric

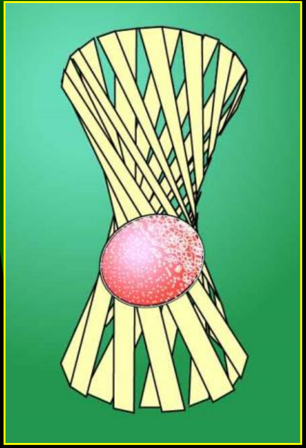
$p^2+1$ mutually noncollinear points

spread in $\mathbb{P}^3\mathbb{F}_p$
gives projective
plane of order $p^2$…

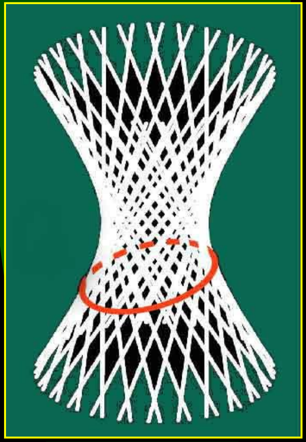
$E_8$ lattice



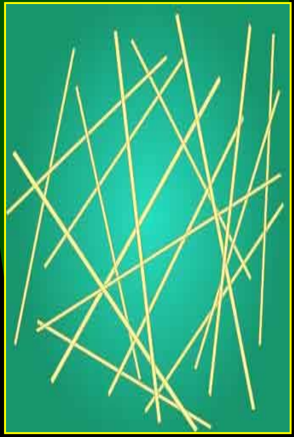
Ovoids
of $P^7\mathbb{F}_p$
quadrics



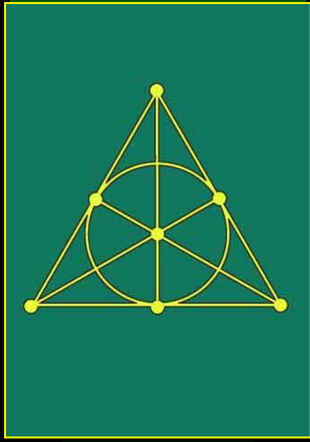
Ovoids
of $P^5\mathbb{F}_p$
quadrics



Spreads
in $\mathbb{P}^3\mathbb{F}_p$

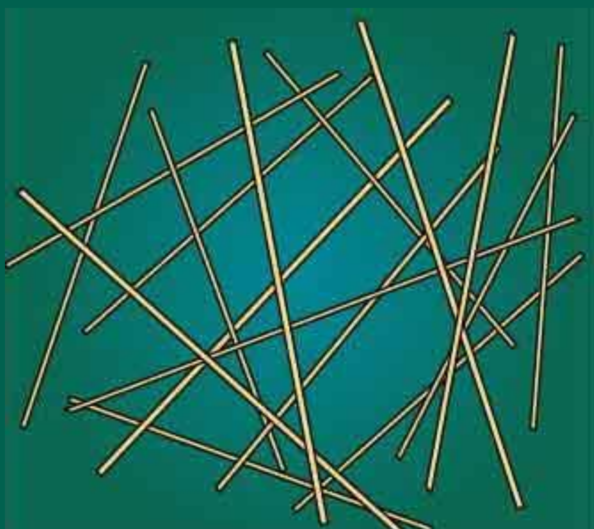


Projective
planes

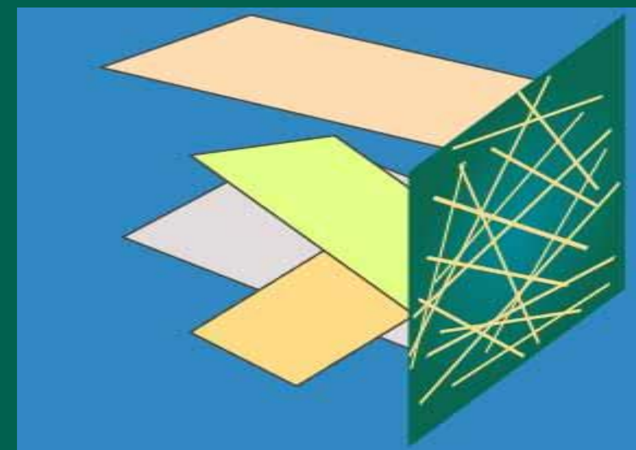


## Spread of 3-space

## Translation plane (affine or projective plane)

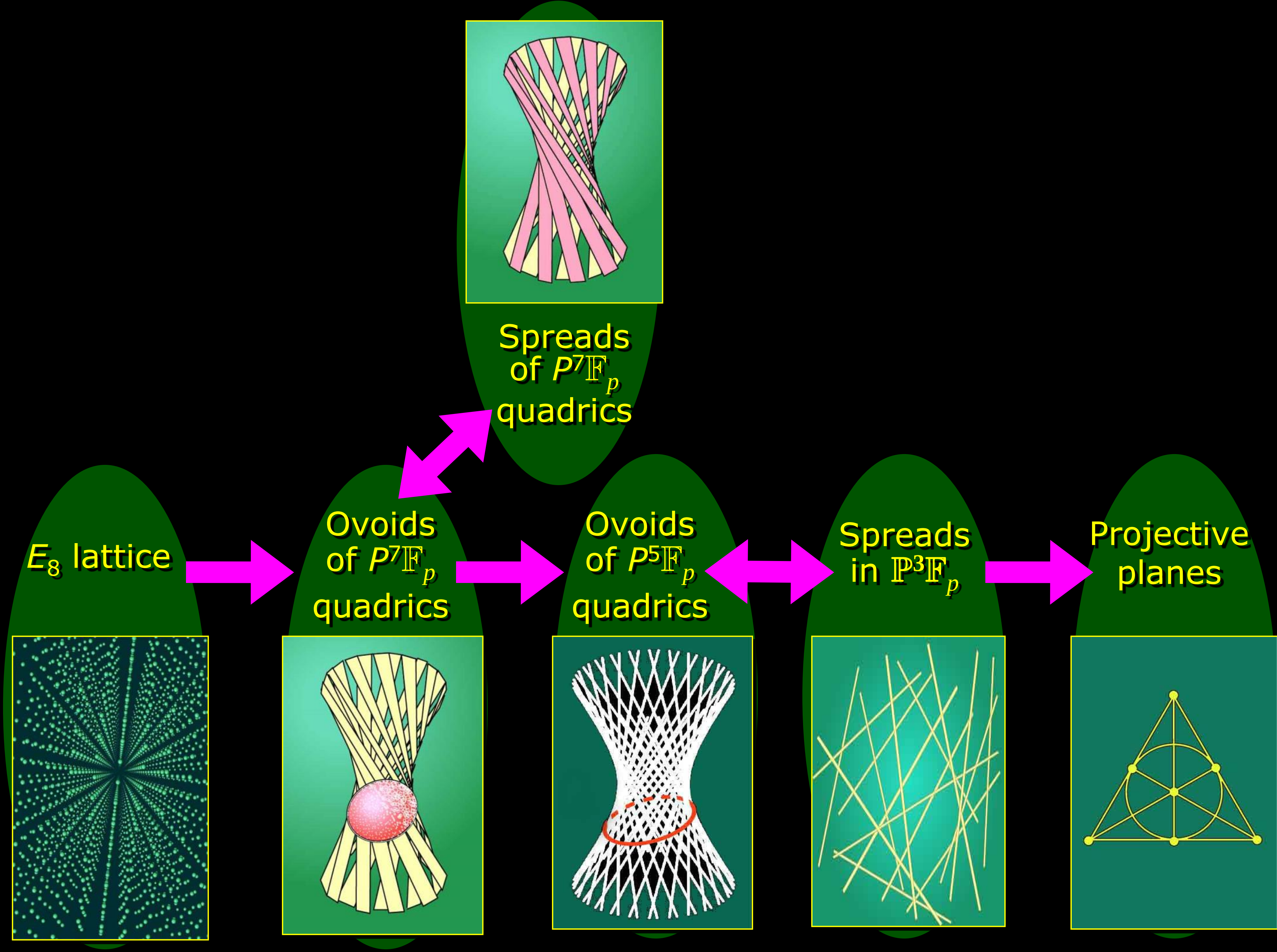


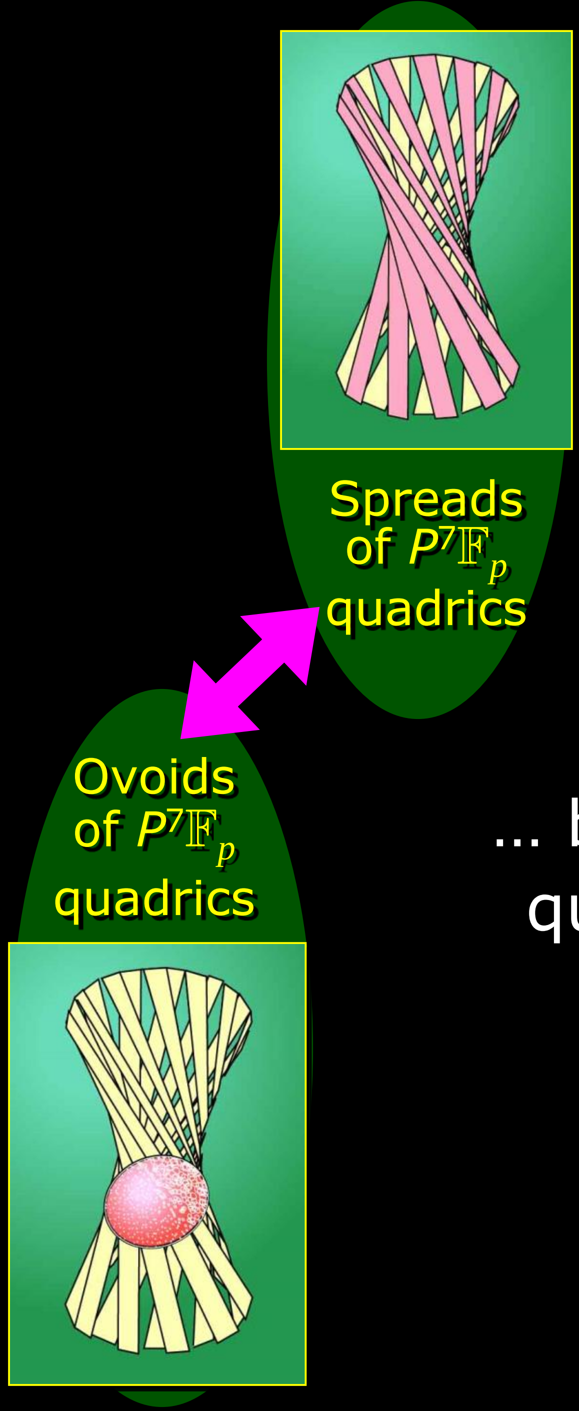
spread of $\mathbb{P}^3\mathbb{F}$, $\mathbb{F} = \mathbb{F}_p$



$p^4$ points: points of $\mathbb{F}^4$

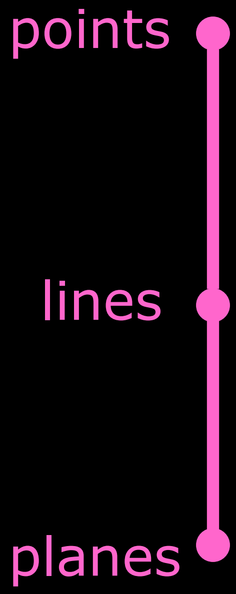
spread at infinity defines the $p^2(p^2+1)$ 'lines' each of size $p^2$


Spreads of $P^7\mathbb{F}_p$ quadrics
$E_8$ lattice
Ovoids of $P^7\mathbb{F}_p$ quadrics
Ovoids of $P^5\mathbb{F}_p$ quadrics
Spreads in $\mathbb{P}^3\mathbb{F}_p$
Projective planes

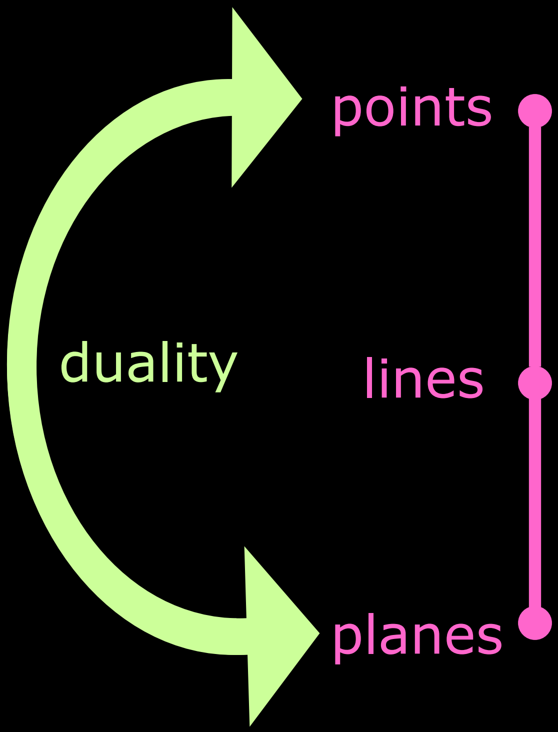


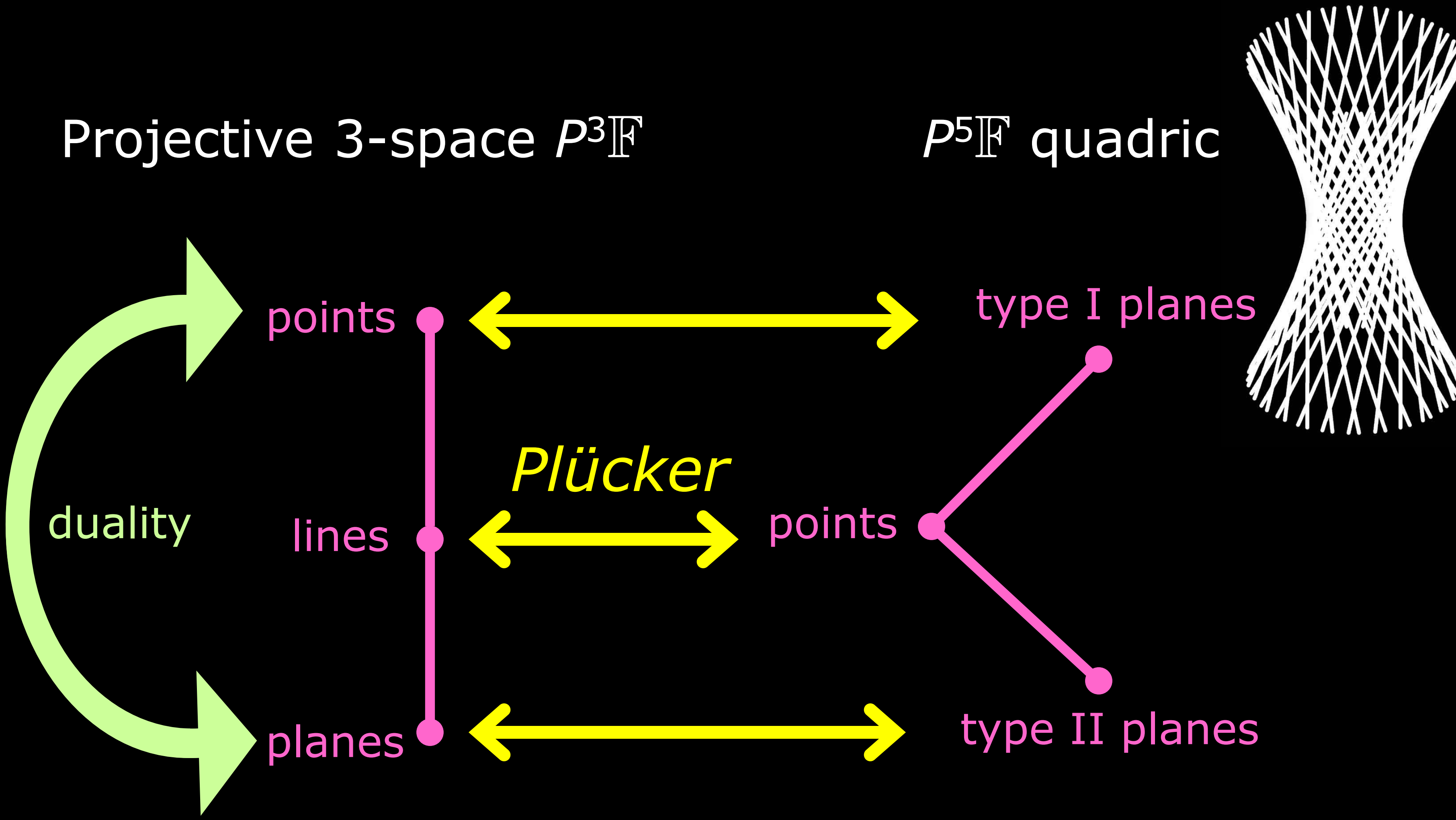

... but first, a proof that $P^5\mathbb{F}$ quadrics have no spreads

# Projective 3-space $P^3\mathbb{F}$

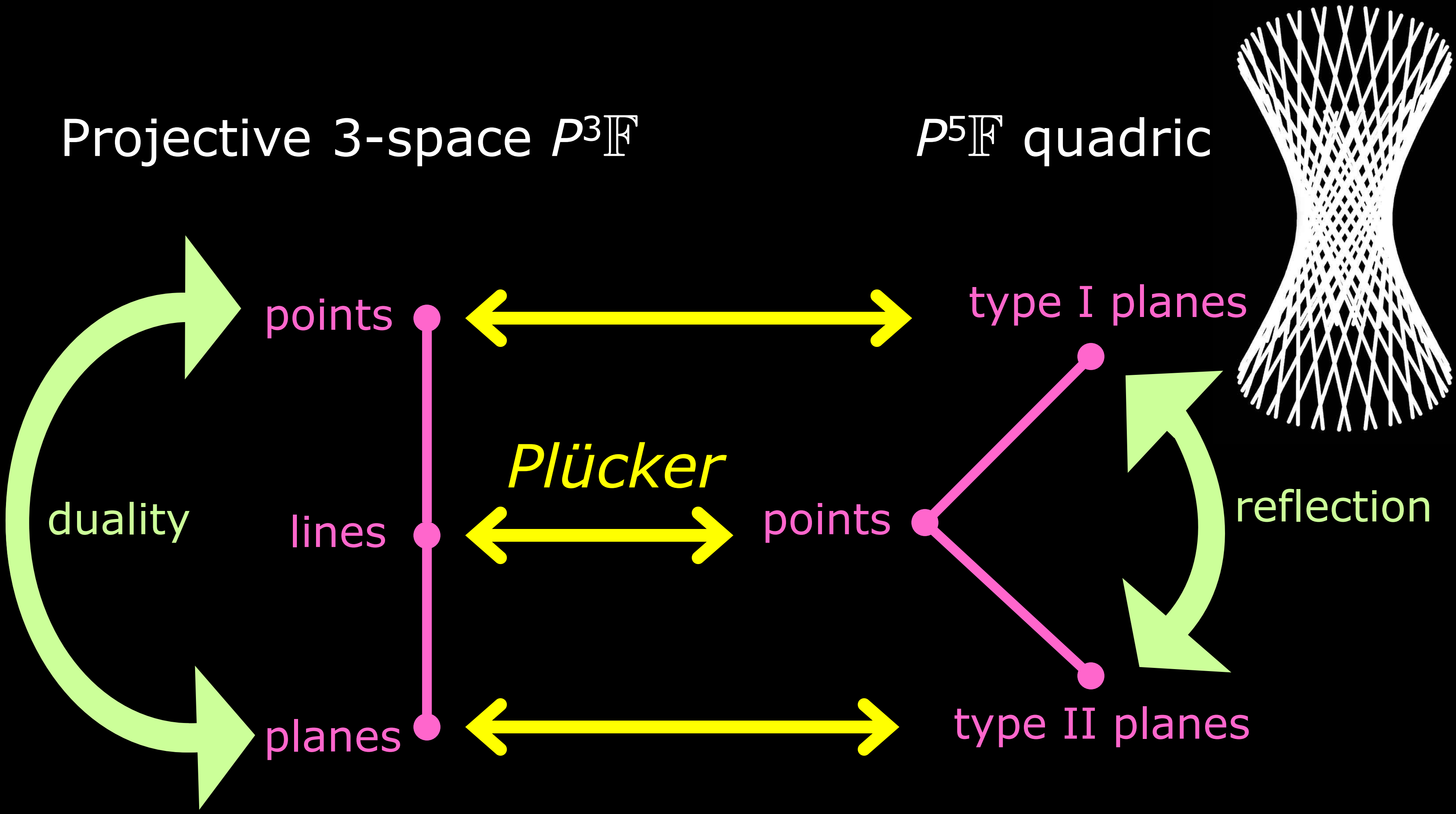


# Projective 3-space $P^3\mathbb{F}$





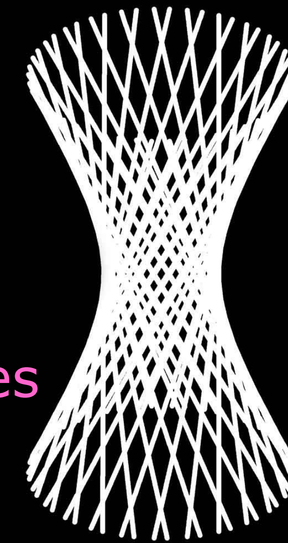
Projective 3-space $P^3\mathbb{F}$
$P^5\mathbb{F}$ quadric
points
lines
planes
duality
Plücker
type I planes
points
type II planes

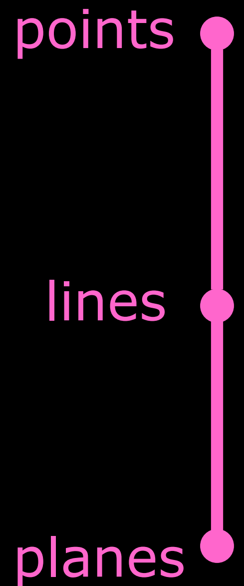


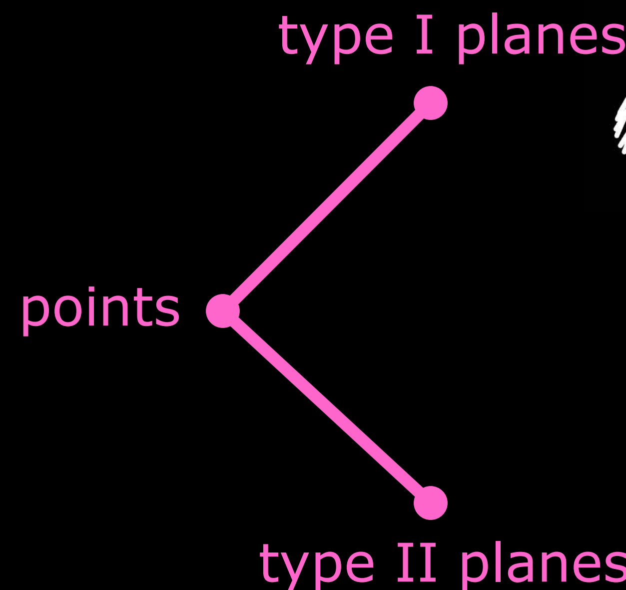
Projective 3-space $P^3\mathbb{F}$
$P^5\mathbb{F}$ quadric
points
lines
planes
duality
Plücker
type I planes
points
type II planes
reflection

Projective 3-space $P^3\mathbb{F}$

$P^5\mathbb{F}$ quadric



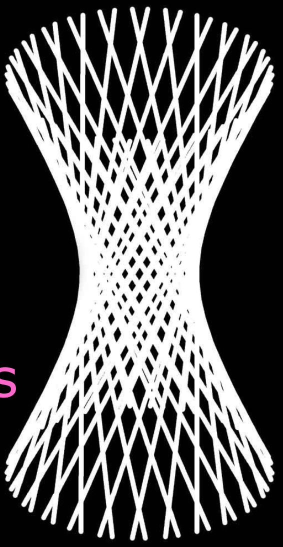


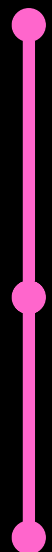



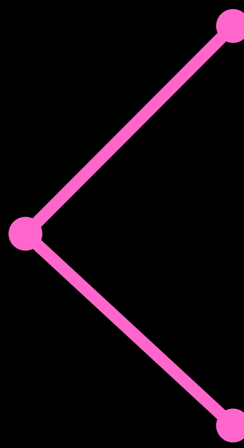

spread

Projective 3-space $P^3\mathbb{F}$

$P^5\mathbb{F}$ quadric





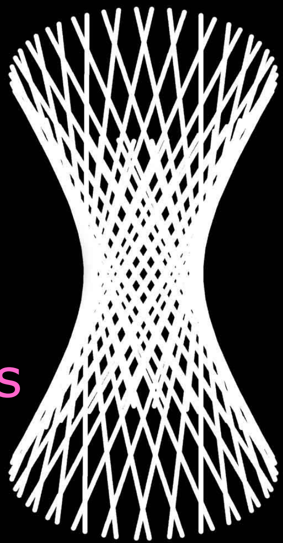




*Plücker*

$p^2$+1 points (or planes), no two collinear ⟷ spread

Projective 3-space $P^3\mathbb{F}$

$P^5\mathbb{F}$ quadric



points

lines

planes

type I planes

points

type II planes

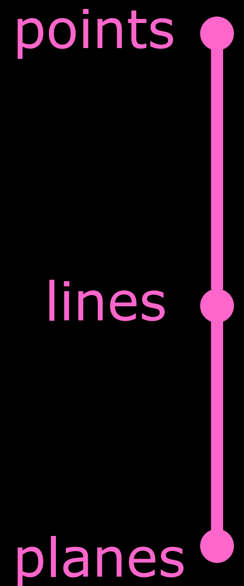
$p^2$+1 points (or planes), no two collinear

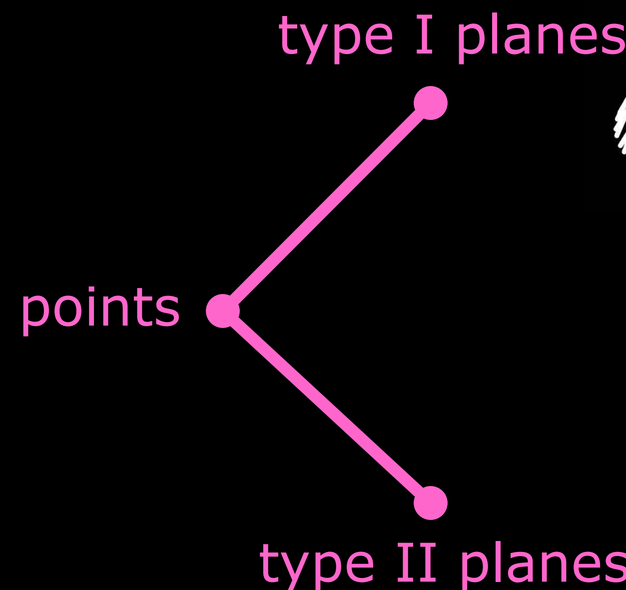
*Plücker*

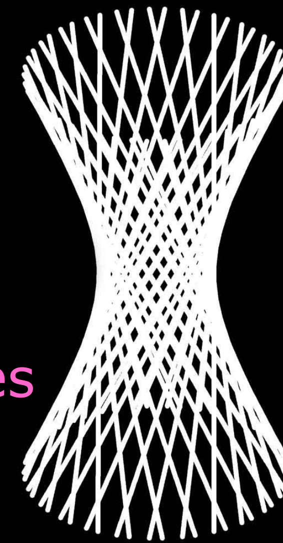
spread

Projective 3-space $P^3\mathbb{F}$

$P^5\mathbb{F}$ quadric



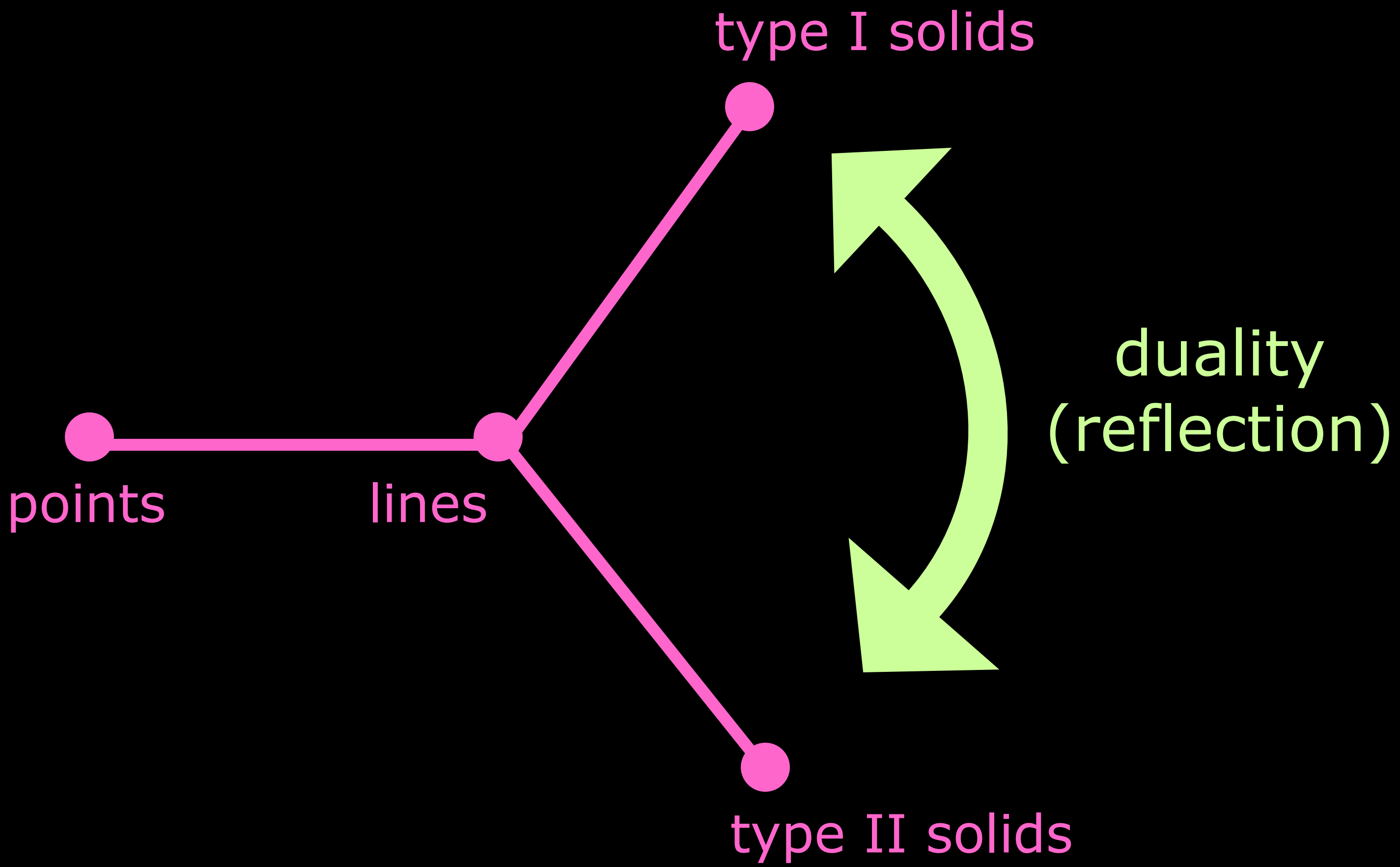



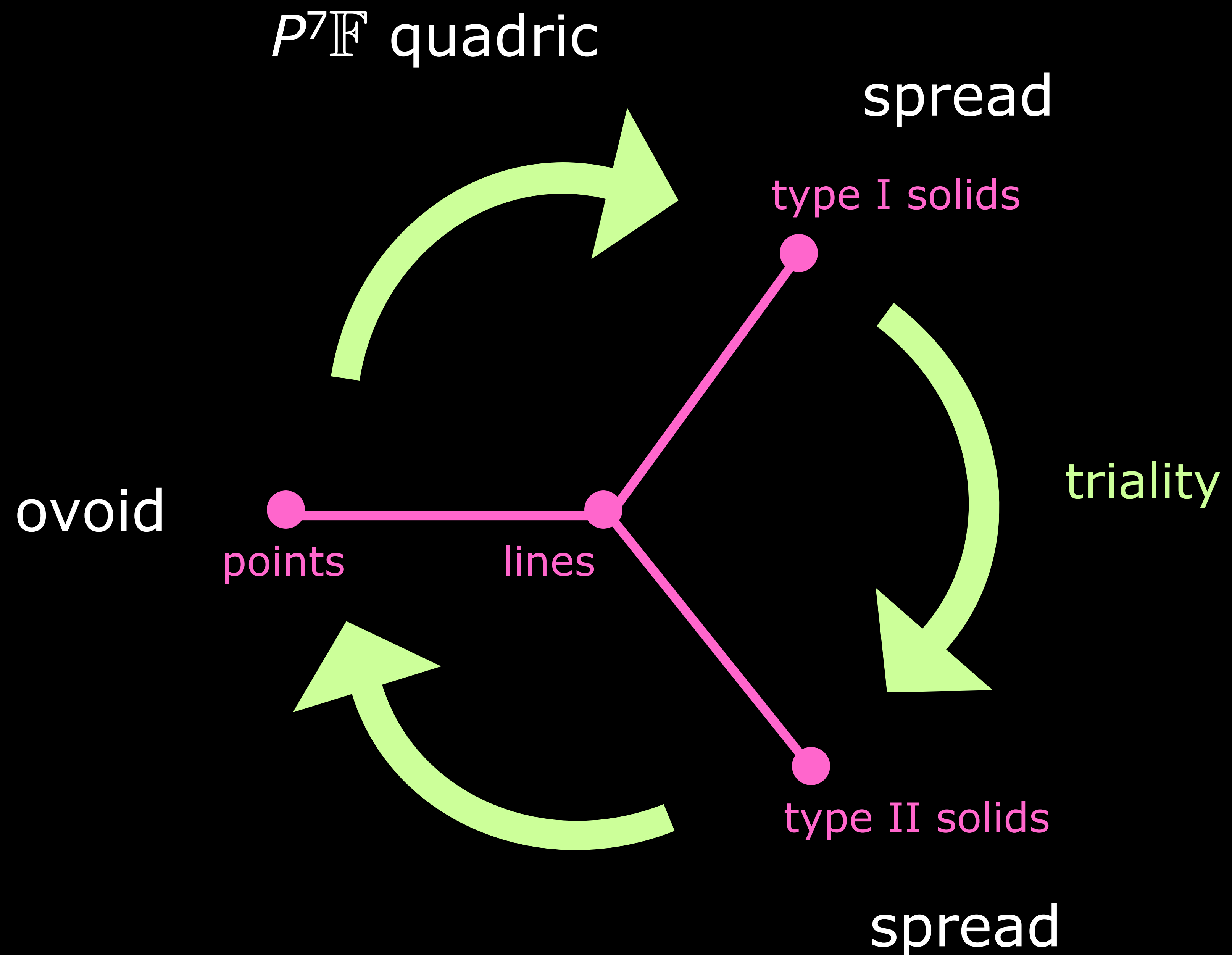
$p^2$+1 points (or planes), no two collinear

*Plücker* ⟷

spread

# $P^7\mathbb{F}$ quadric

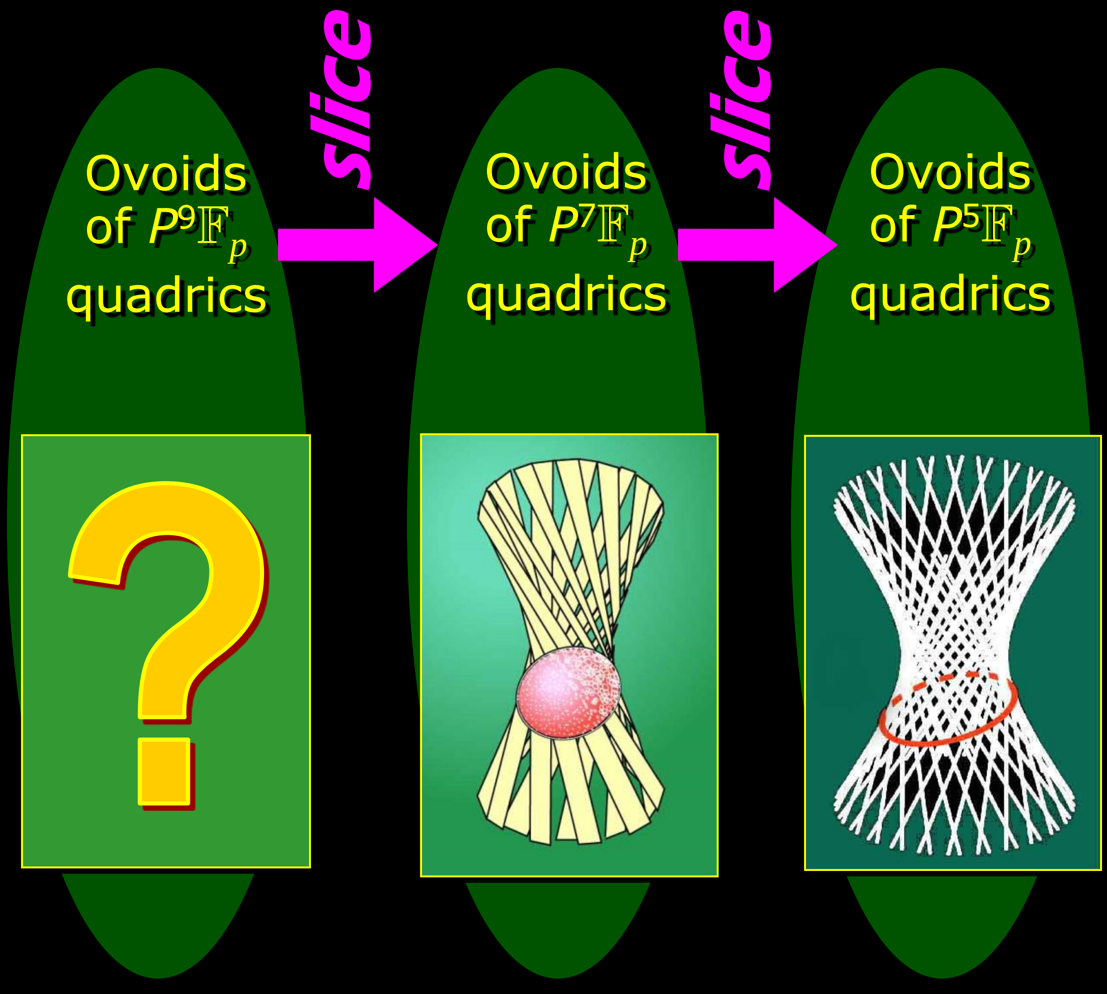




$P^7\mathbb{F}$ quadric
spread
type I solids
triality
ovoid
points
lines
type II solids
spread

*No 9-dimensional ovoids are known!*

# No 9-dimensional ovoids are known!




*Is the apparent lack of ovoids in $P^9\mathbb{F}_p$ due to a lack of dense lattices in $\mathbb{R}^{10}$ ?*

Try to generalise this to ovoids over $\mathbb{F}_{p^k}$:

$$E_8/pE_8 \cong \mathbb{F}_p^8$$

Let $\mathcal{A}$ be the ring of algebraic integers in a number field of degree $k$ over $\mathbb{Q}$.

$L = E_8 \otimes_{\mathbb{Z}} \mathcal{A}$ is a lattice over $\mathcal{A}$; $\quad L/pL \cong \mathbb{F}_{p^k}^{\,8}$

Try to choose vectors in shells of $L$ and reduce mod $p$ to get ovoids.

This fails!

*Lubotzky, Phillips and Sarnak (1988):*

Explicit construction of Ramanujan graphs (sparse but highly connected graphs) using theta series of $\mathbb{Z}^4 = A_1 \oplus A_1 \oplus A_1 \oplus A_1$:

$$\Theta(z) = 1 + 8\Big(\sum_{\substack{d \mid m \\ d \neq 0 \bmod 4}} d\Big) q^m$$

For odd primes $p$, the coefficient of $q^p$ is $8(p+1)$ (but this exact value is not required, only its rate of growth).