

# Approaching Some Problems in Finite Geometry Through Algebraic Geometry

Eric Moorhouse

UNIVERSITY OF WYOMING

<http://www.uwyo.edu/moorhouse/>

## Algebraic Combinatorics

- finite geometry (classical and nonclassical)
- association schemes
- algebraic graph theory
- combinatorial designs
- enumerative combinatorics (à la Rota, Stanley, etc.)
- much more...

Use of Gröbner Bases: Conceptual vs. Computational

## Outline

1. Motivation / Background from Finite Geometry
2.  $p$ -ranks
3. Computing  $p$ -ranks via the Hilbert Function
4. Open Problems



# 1. Motivation / Background from Finite Geometry

*Classical projective  $n$ -space  $P^n_{\mathbb{F}_q}$ :*

incidence system formed by subspaces of  $\mathbb{F}_q^{n+1}$

*points* = 1-spaces

*lines* = 2-spaces

*planes* = 3-spaces

etc.

Non-classical projective planes (2-spaces) exist  
but spaces of dimension  $\geq 3$  are classical

## 1. Motivation / Background from Finite Geometry

An *ovoid* in projective 3-space  $P^3\mathbb{F}_q$ :  
a set  $\mathcal{O}$  consisting of  $q^2+1$  points, no three collinear.

Let  $\mathcal{C}$  be a linear  $[n,4]$  code over  $\mathbb{F}_q$ .

If  $\mathcal{C}^\perp$  has minimum weight  $\geq 4$  then  $n \leq q^2+1$ .

When equality occurs then a generator matrix  $G$  for  $\mathcal{C}$  has as its columns an ovoid.

## 1. Motivation / Background from Finite Geometry

An *ovoid* in projective 3-space  $P^3\mathbb{F}_q$ :  
a set  $\mathcal{O}$  consisting of  $q^2+1$  points, no three collinear.

For  $q$  odd, an ovoid is an *elliptic quadric* [Barlotti (1955);  
Panella (1955)].

When  $q$  is even the *known* ovoids are the elliptic  
quadrics, and (when  $q=2^{2e+1}$ ) the *Suzuki-Tits ovoids*.

## 1. Motivation / Background from Finite Geometry

A *spread* in projective  $(2n-1)$ -space  $P^{2n-1}\mathbb{F}_q$ :  
a set  $\mathcal{S}$  consisting of  $q^n+1$  projective  $(n-1)$ -subspaces,  
partitioning the points of  $(2n-1)$ -space.

These exist for all  $n$  and  $q$ , and give rise to  
*translation planes* (the most prolific source of  
non-classical projective planes).

## 1. Motivation / Background from Finite Geometry

*Classical polar spaces of orthogonal, unitary, symplectic type :*

projective subspaces of  $P^n_{\mathbb{F}_q}$  totally singular/isotropic with respect to the appropriate form, which induces a polarity

*Orthogonal polar space:* nondegenerate quadric

*Unitary polar space:* Hermitian variety

Projective and polar spaces constitute the Lie incidence geometries of types  $A_n, B_n, C_n, D_n$



## 1. Motivation / Background from Finite Geometry

*Ovoid of a polar space  $\mathcal{P}$ :*

a point set  $\mathcal{O}$  meeting every maximal subspace of  $\mathcal{P}$  exactly once

*Spread of a polar space  $\mathcal{P}$ :*

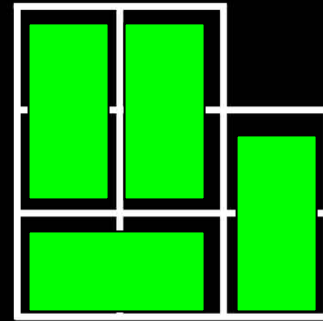
a partition  $\mathcal{S}$  of the point set into maximal subspaces

Many existence questions for ovoids and spreads remain open.

These may be regarded as dual packing problems:

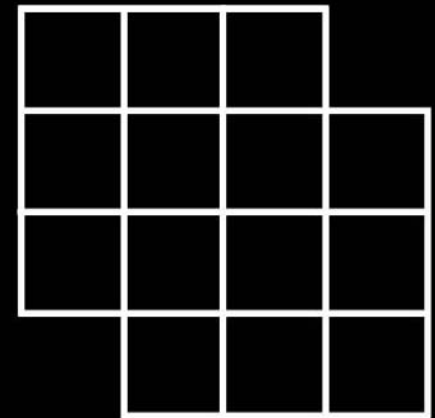
# Sample Packing Problem

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



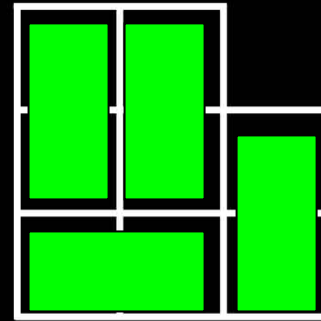
One, of several, solutions.  
Such a complete tiling we'll call a *spread*.

This figure  
has *no spread* of dominoes:



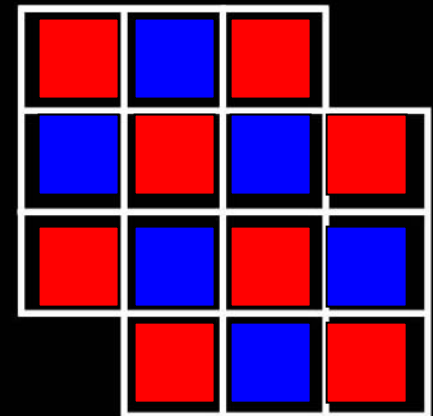
# Sample Packing Problem

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



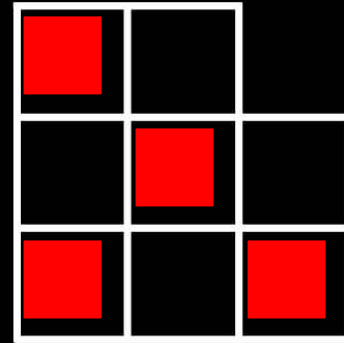
One, of several, solutions.  
Such a complete tiling we'll call a *spread*.

This figure  
has *no spread* of dominoes:



# The Dual Packing Problem

Find a set of cells meeting each domino exactly once.

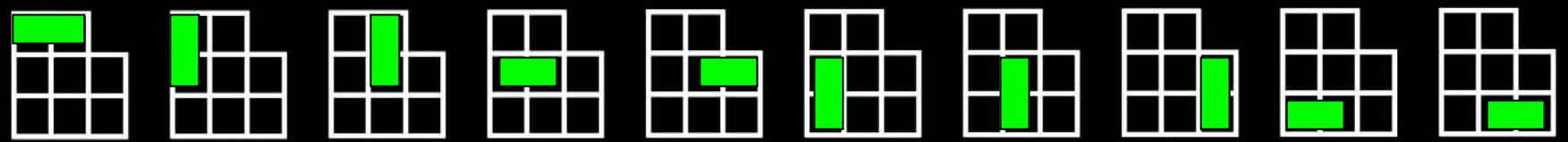
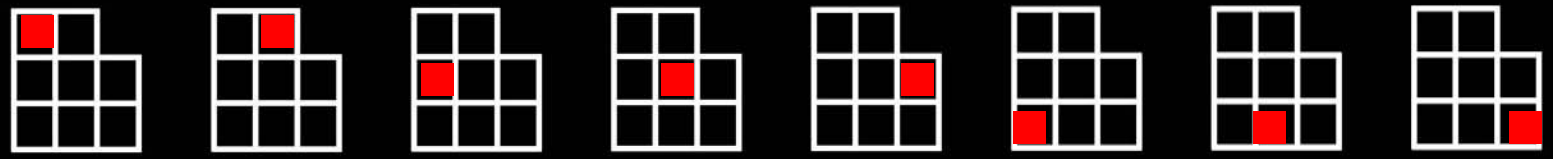


One of two solutions.

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

Why is this problem dual to the previous one?

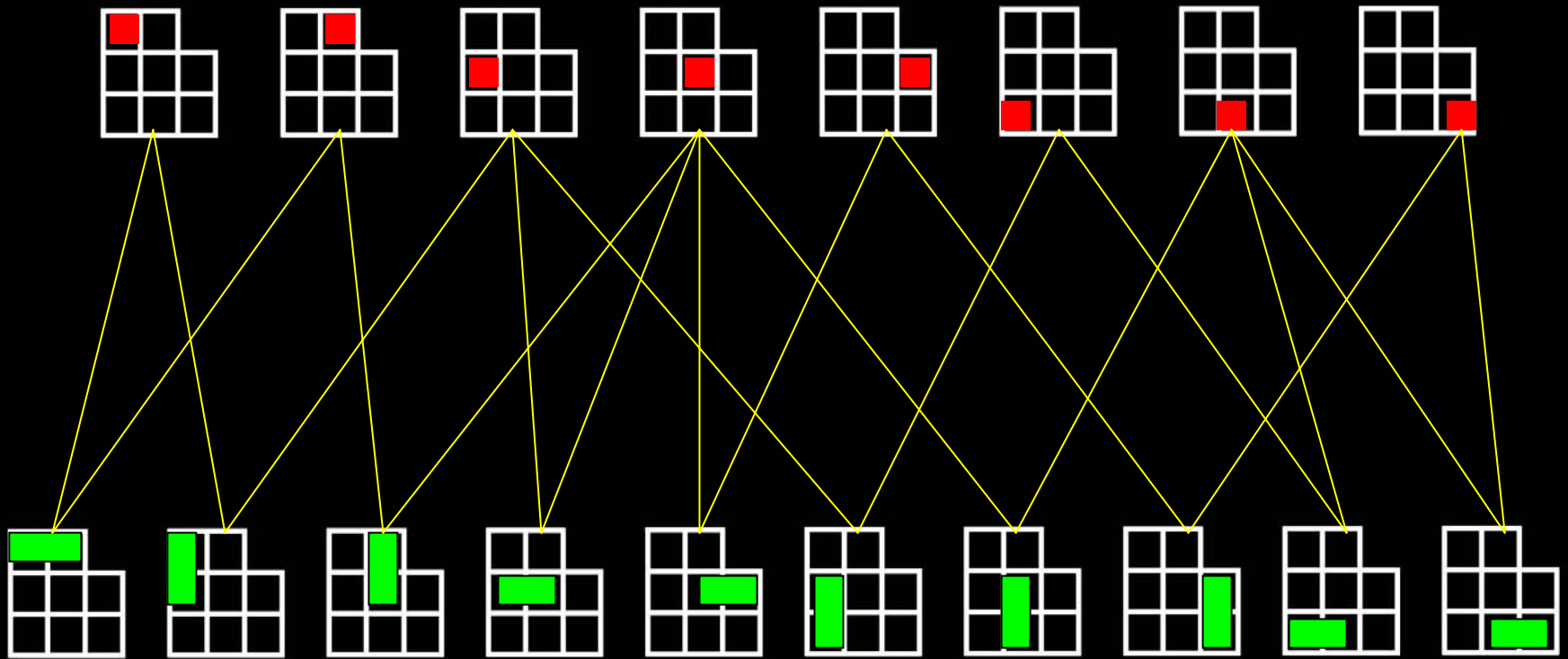
**“Points” (cells)**



**“Lines” (dominoes)**

# *bipartite graph:*

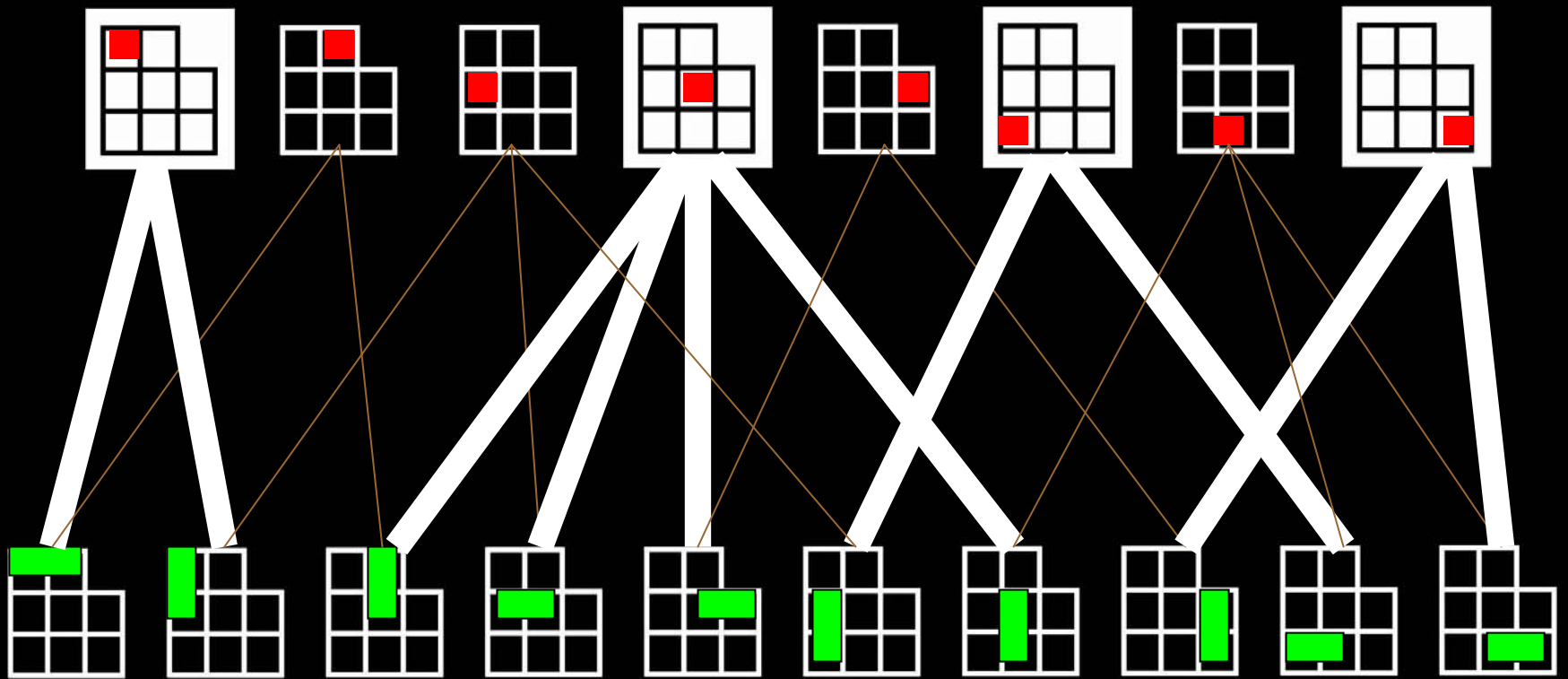
“Points” (cells)



“Lines” (dominoes)

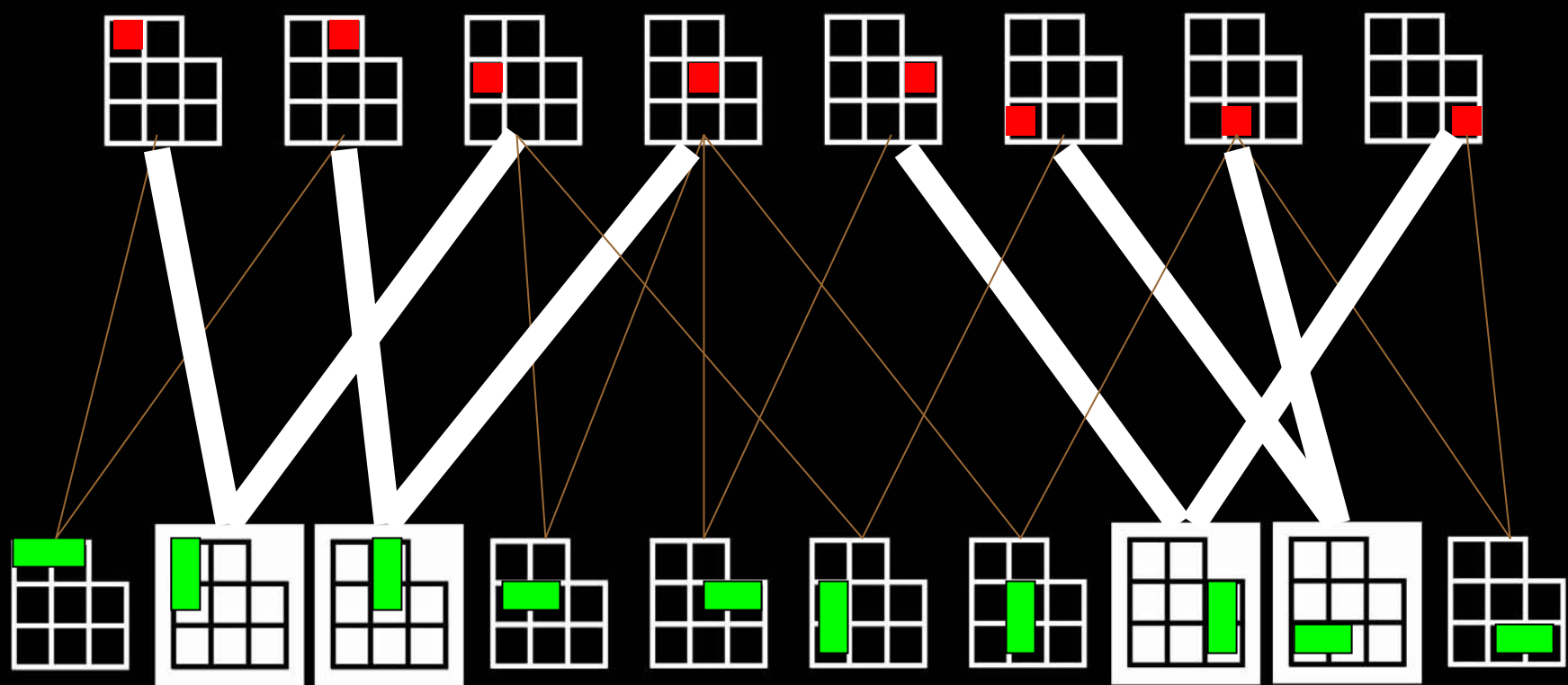
# *Ovoid*

“Points” (cells)



“Lines” (dominoes)

“Points” (cells)

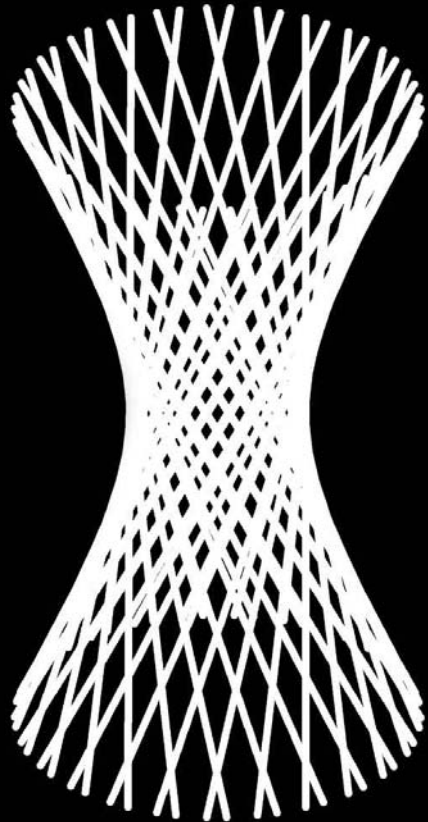


“Lines” (dominoes)

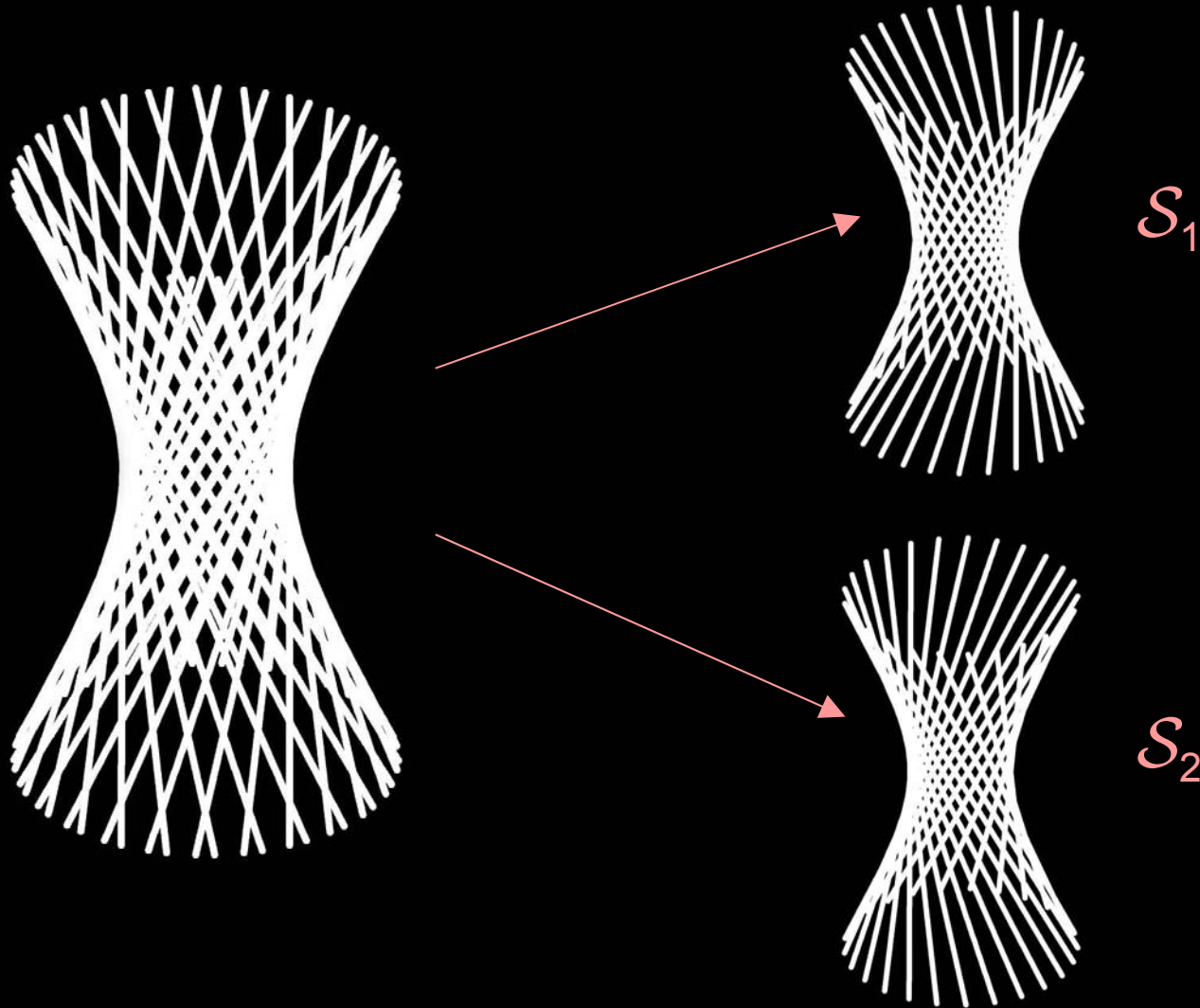
*Spread*



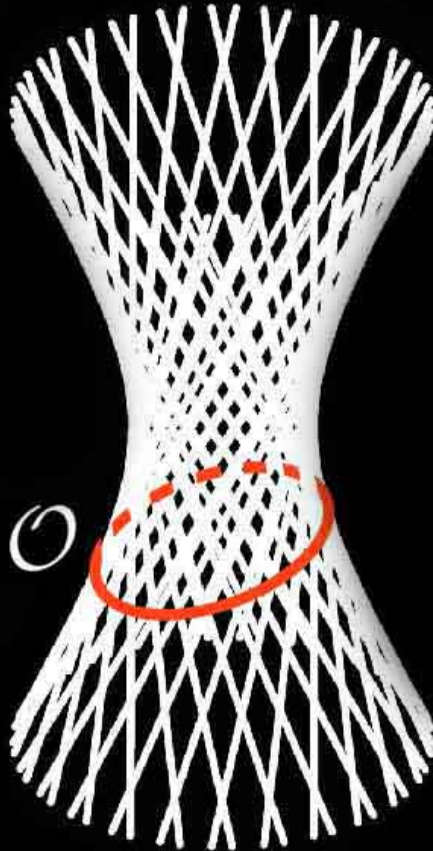
Hyperbolic (i.e. ruled) quadrics in  $P^3F$



Hyperbolic (i.e. ruled) quadrics in  $P^3F$  have spreads

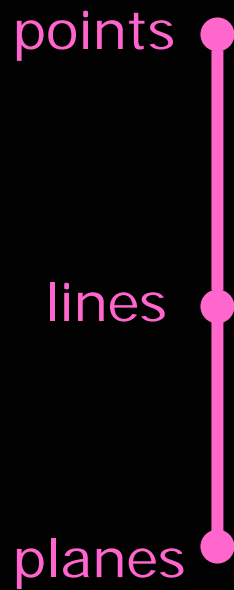


Hyperbolic (i.e. ruled) quadrics in  $P^3F$  have ovoids



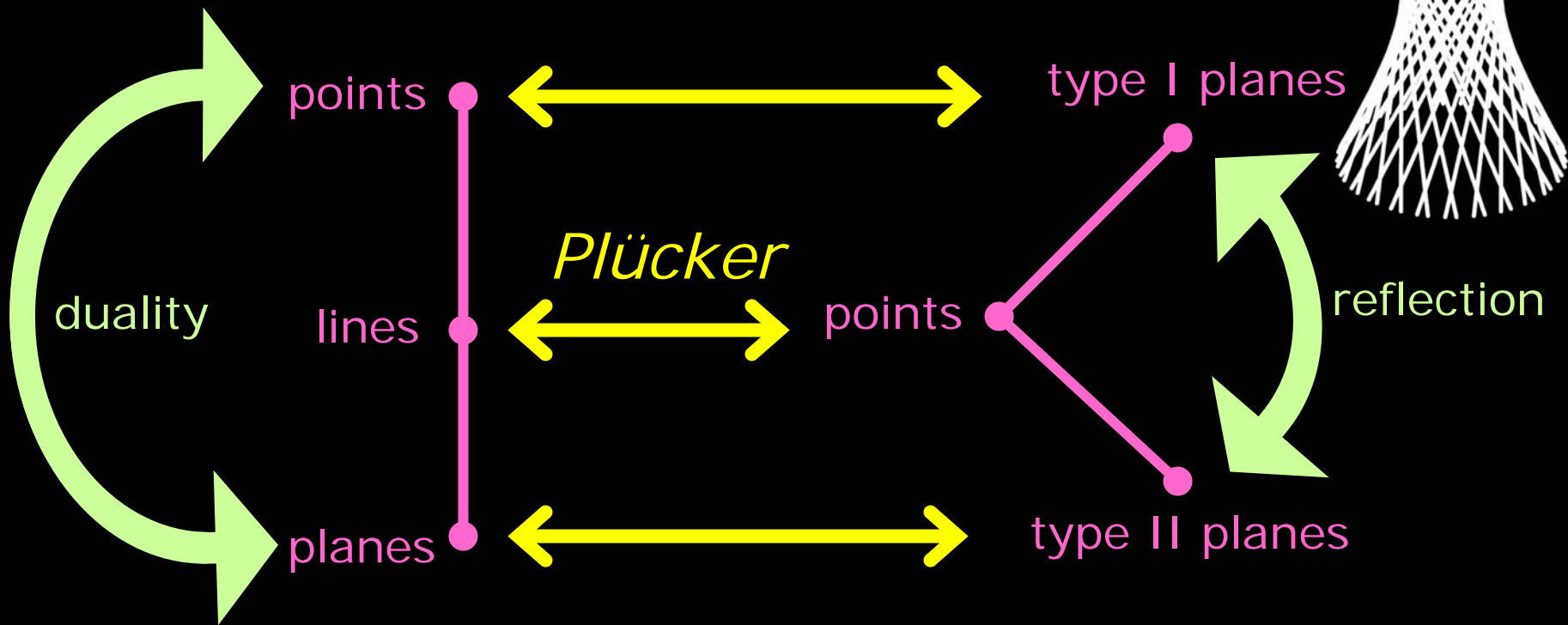
All real quadrics have ovoids. Some have spreads.

# Projective 3-space $P^3F$



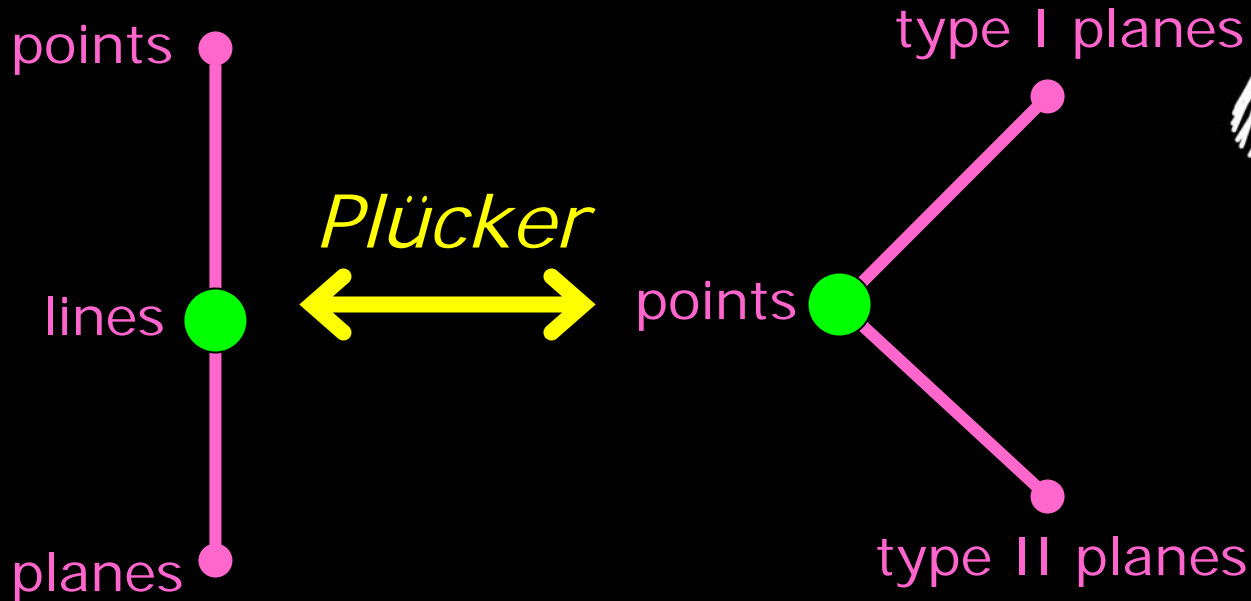
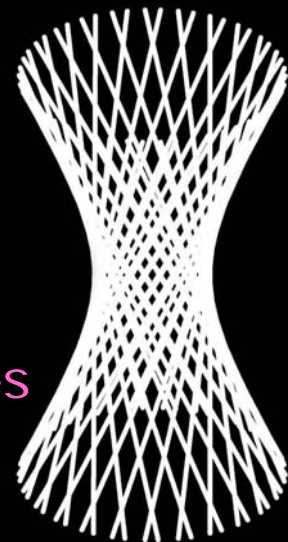
Projective 3-space  $P^3F$

$P^5F$  quadric



Projective 3-space  $P^3F$

$P^5F$  quadric



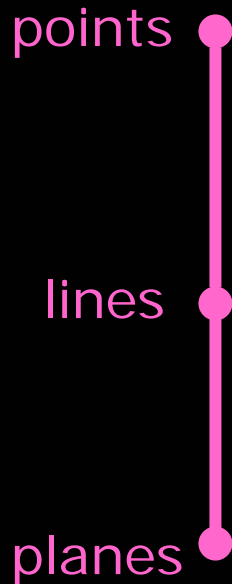
spread:

$q^2+1$  lines,  
pairwise disjoint

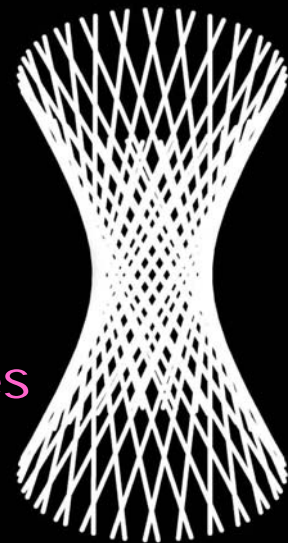
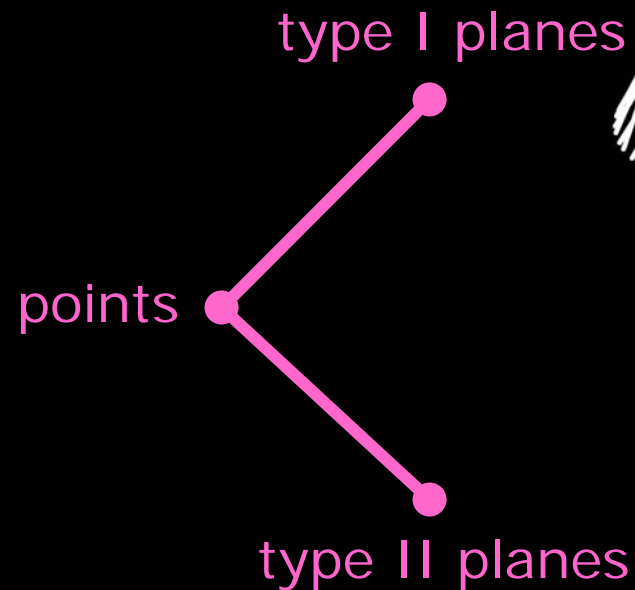
ovoid:

$q^2+1$  points,  
no two collinear

Projective 3-space  $P^3F$

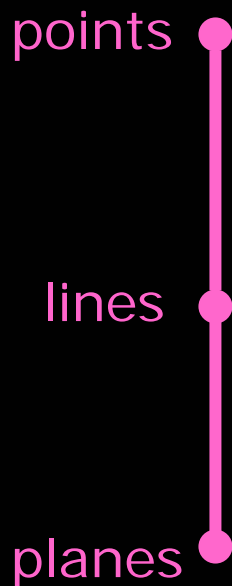


$P^5F$  quadric



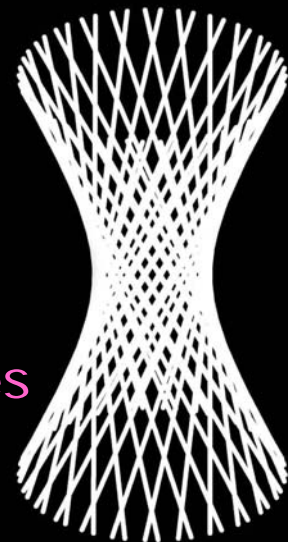
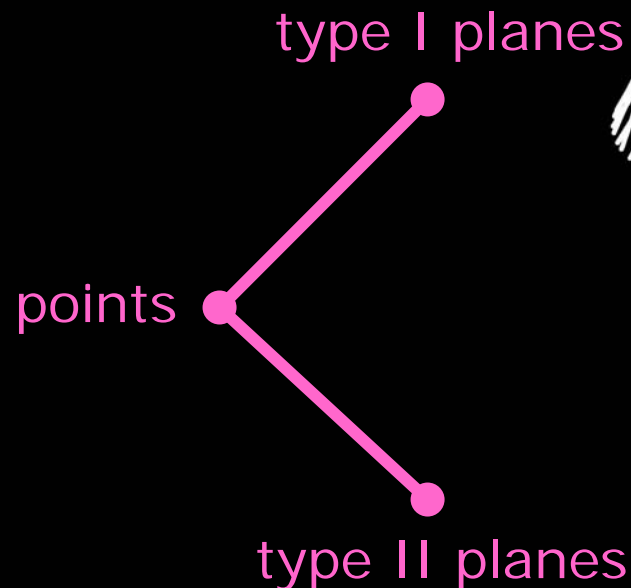
spread

Projective 3-space  $P^3F$



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

$P^5F$  quadric



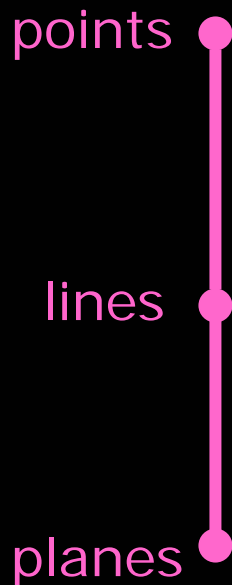
*Plücker*



spread

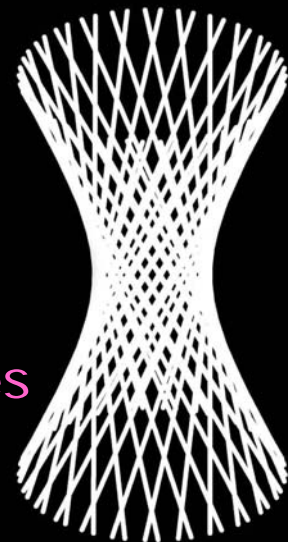
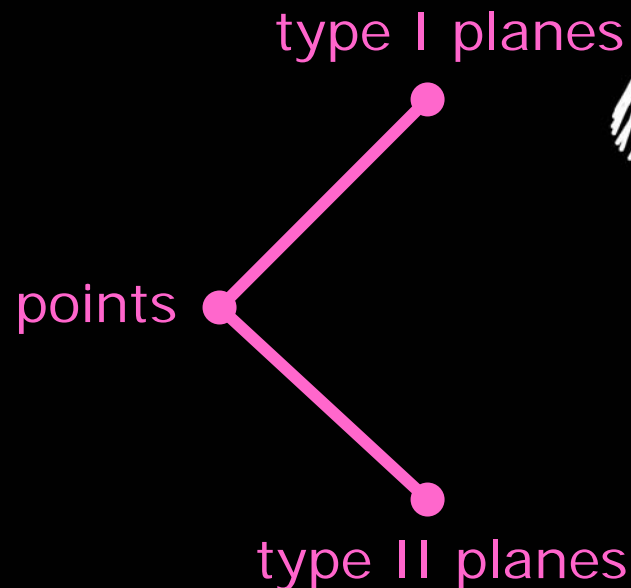


Projective 3-space  $P^3F$



~~$q^2 + 1$  points (or planes) no two collinear~~

$P^5F$  quadric

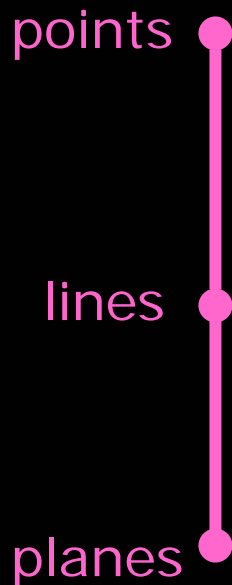


*Plücker*



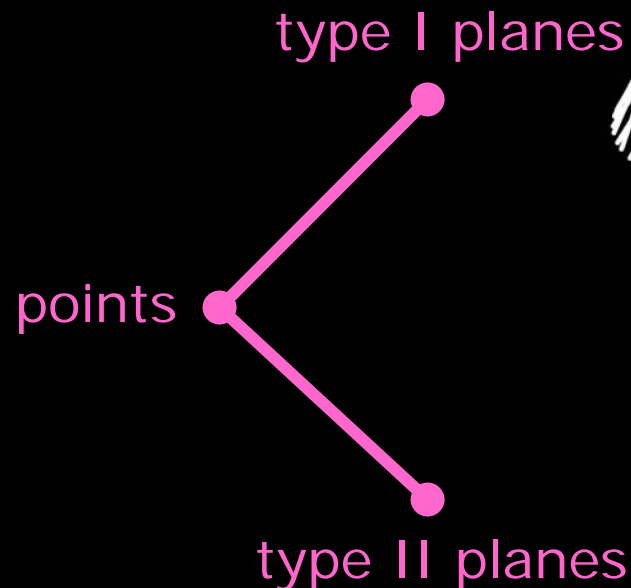
spread

Projective 3-space  $P^3F$

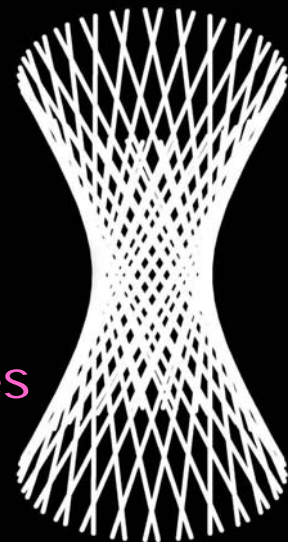


~~$q^2 + 1$  points (or planes) no two collinear~~

$P^5F$  quadric



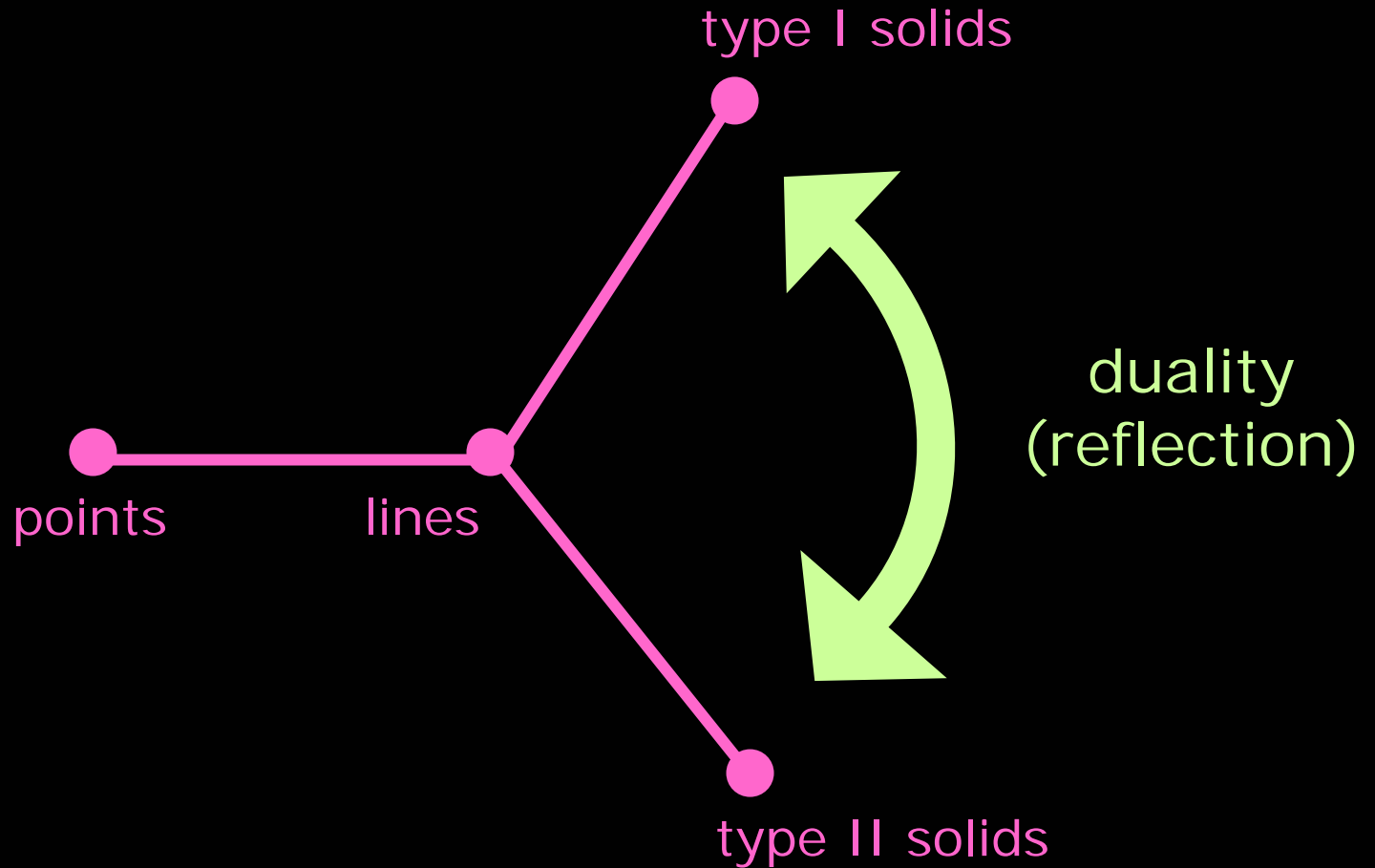
~~spread~~



*Plücker*



# $P^7 F$ quadric



$P^7 F$  quadric

spread

type I solids

trinality

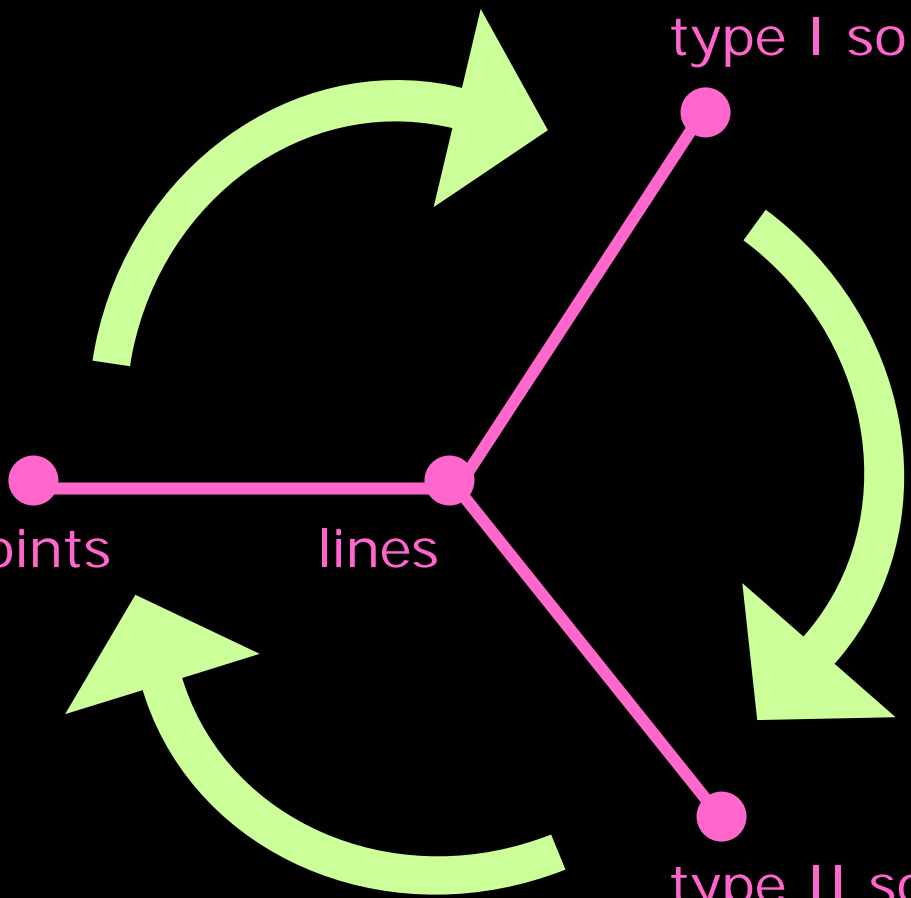
ovoid

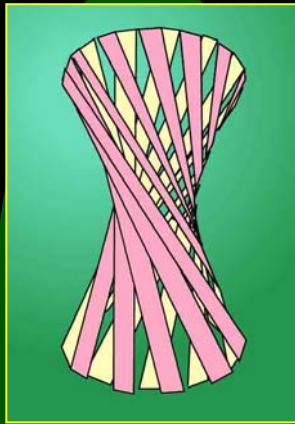
points

lines

type II solids

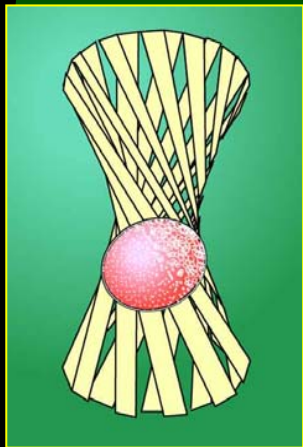
spread



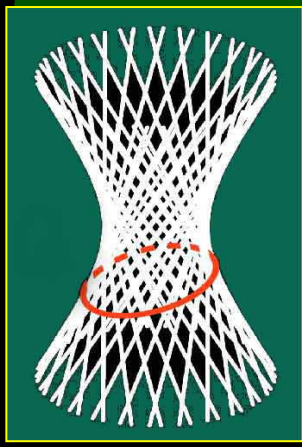


Spreads  
of  $P^1 F$   
quadrics

Ovoids  
of  $P^1 F$   
quadrics



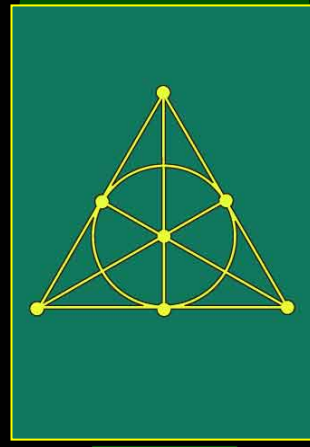
Ovoids  
of  $P^5 F$   
quadrics



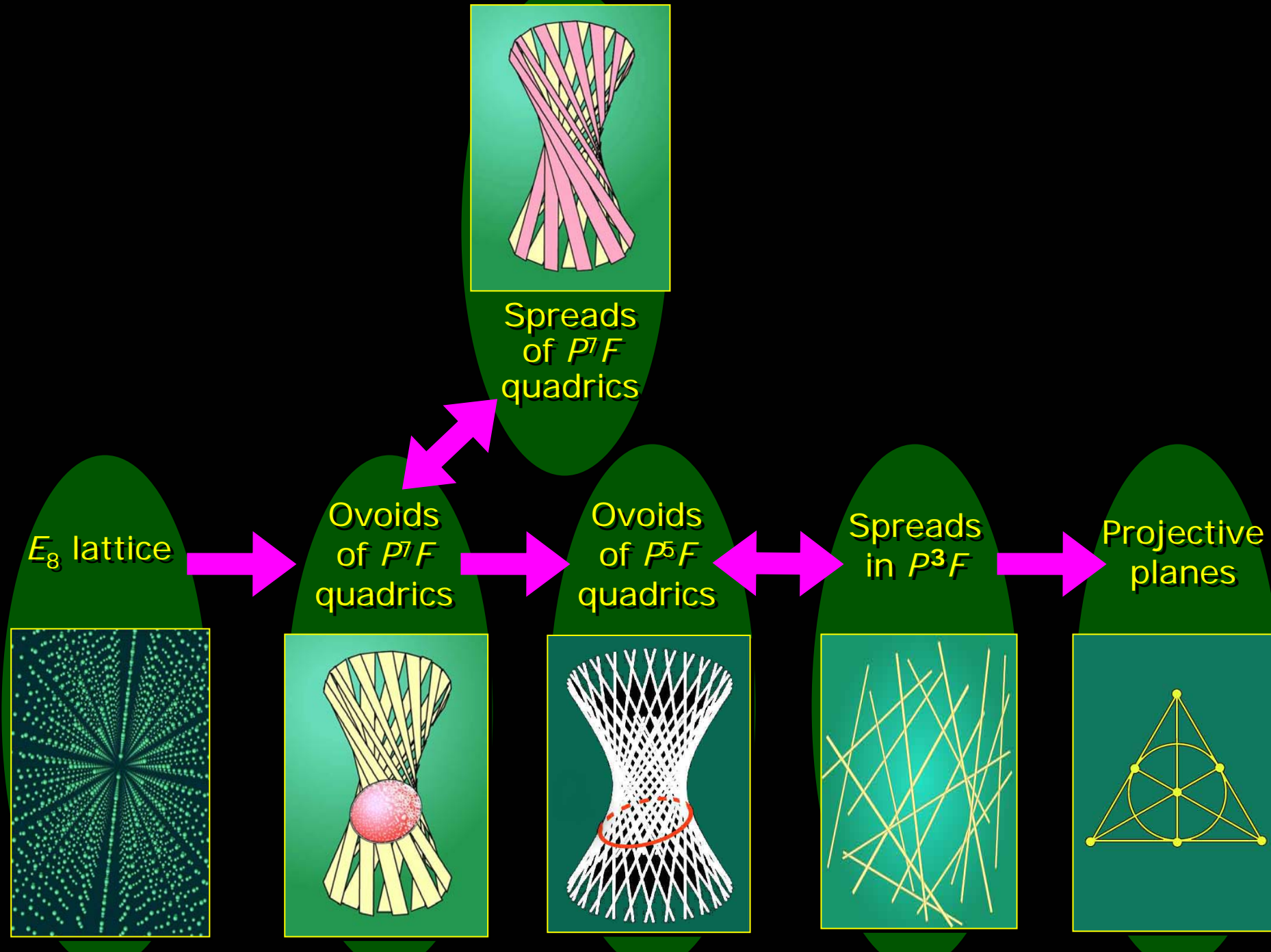
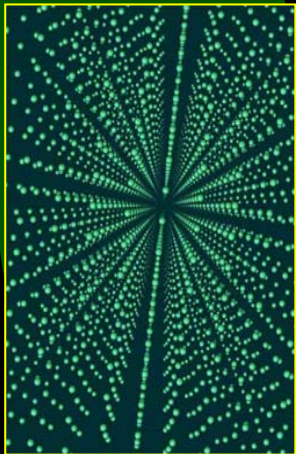
Spreads  
in  $P^3 F$



Projective  
planes



$E_8$  lattice



Ovoids in  $P^3\mathbb{F}_q$ ,  
 $q=2^r$

Known examples:

- Elliptic quadrics  
admitting  $PSL(2, q^2)$
- ( $r$  odd) Suzuki-Tits ovoids  
admitting  ${}^2B_2(q)$

Code spanned by planes  
has dimension  $q^2+1$ .

Basis:  $p^\perp$ ,  $p \in \mathcal{O}$

$$|\mathcal{O}| = q^2+1$$

Ovoids in  
quadrics of  $P^7\mathbb{F}_q$ ,  
 $q=2^r$

Known examples:

- Examples  
admitting  $PSL(3, q)$
- ( $r$  odd) Examples  
admitting  $PSU(3, q)$
- ( $q=8$ ) sporadic  
example

Code spanned by  
tangent hyperplanes  
to quadric  
has dimension  $q^3+1$ .

Basis:  $p^\perp$ ,  $p \in \mathcal{O}$

$$|\mathcal{O}| = q^3+1$$

Ovoids in  
quadrics of  $P^6\mathbb{F}_q$ ,  
 $q=3^r$

Known examples:

- Examples  
admitting  $PSU(3, q)$
- ( $r$  odd) Ree-Tits ovoids  
admitting  ${}^2G_2(q)$

Code spanned by  
tangent hyperplanes  
to quadric  
has dimension  $q^3+1$ .

Basis:  $p^\perp$ ,  $p \in \mathcal{O}$

$$|\mathcal{O}| = q^3+1$$

## Ovoids in quadrics of $P^n \mathbb{F}_q$ , $q=p^r$

- *always* exist for  $n=7$  and  $r=1$  (use  $E_8$  root lattice)  
[J.H. Conway et. al. (1988); M. (1993)]
- do *not* exist for  $p^{\lfloor n/2 \rfloor} > \binom{p+n-1}{n} - \binom{p+n-3}{n}$   
[Blokhuis and M. (1995)]

e.g. ovoids do not exist

- for  $n=9$ ,  $p=2,3$ ;
- for  $n=11$ ,  $p=2,3,5,7$ ; etc.

Code spanned by tangent hyperplanes to quadric has dimension

$$\left[ \binom{p+n-1}{n} - \binom{p+n-3}{n} \right]^r + 1$$

Subcode spanned by tangent hyperplanes to putative ovoid has dimension

$$|\mathcal{O}| = p^{\lfloor n/2 \rfloor} r + 1$$

## Ovoids in quadrics of $P^n \mathbb{F}_q$ , $q=p^r$

- *always* exist for  $n=7$  and  $r=1$  (use  $E_8$  root lattice)  
[J.H. Conway et. al. (1988); M. (1993)]
- do *not* exist for  $p^{\lfloor n/2 \rfloor} > \binom{p+n-1}{n} - \binom{p+n-3}{n}$   
[Blokhuis and M. (1995)]  
  
e.g. ovoids do not exist
  - for  $n=9$ ,  $p=2,3$ ;
  - for  $n=11$ ,  $p=2,3,5,7$ ; etc.
- do *not* exist for  $n=8,10,12,14,16,\dots$   
[Gunawardena and M. (1997)]

Similar results for ovoids on Hermitian varieties  
[M. (1996)]



## 2. $p$ -ranks

$$F = \mathbb{F}_q, \quad q = p^r$$

$$N = (q^{n+1} - 1)/(q - 1) = \text{number of points of } P^n F$$

The code over  $F = \mathbb{F}_q$  spanned by (characteristic vectors of) hyperplanes of  $P^n F$  has dimension

$$\binom{p+n-1}{n}^r + 1$$

[Goethals and Delsarte (1968); MacWilliams and Mann (1968); Smith (1969)]

Stronger information: Smith Normal Form of point-hyperplane adjacency matrix [Black and List (1990)]

## 2. $p$ -ranks

$$F = \mathbb{F}_q, \quad q = p^r$$

$$N = (q^{n+1} - 1)/(q - 1) = \text{number of points of } P^n F$$

More generally, let  $\mathcal{C} = \mathcal{C}(n, k, p, r)$  be the code over  $F$  of length  $N$  spanned by projective subspaces of codimension  $k$ . Then

$$\dim \mathcal{C} = 1 + \left( \text{coeff. of } t^r \text{ in } \text{tr}([I - tA]^{-1}) \right)$$

where  $A$  is the  $k \times k$  matrix with  $(i, j)$ -entry equal to the coefficient of  $t^{pj-i}$  in  $(1 + t + t^2 + \dots + t^{p-1})^{n+1}$ .

Original formula for  $\dim \mathcal{C}$  due to Hamada (1968).

This improved form is implicit in Bardoe and Sin (2000).

Smith Normal Form: Chandler, Sin and Xiang (2006).

## 2. $p$ -ranks

$$F = \mathbb{F}_q, \quad q = p^r$$

$Q$ : nondegenerate quadric in  $P^4 F$

$$N = (q^4 - 1)/(q - 1) = \text{number of points of } Q$$

$\mathcal{C} = \mathcal{C}(n, p, r)$  = the code over  $F = \mathbb{F}_q$  of length  $N$  spanned by (characteristic vectors of) lines which lie on  $Q$

$$\dim \mathcal{C} = \begin{cases} 1 + \left(\frac{1 + \sqrt{17}}{2}\right)^{2r} + \left(\frac{1 - \sqrt{17}}{2}\right)^{2r}, & p=2 & \text{[Sastry and Sin (1996)];} \\ 1 + \frac{p(p+1)^2}{2}, & q=p & \text{[de Caen and M. (1998)];} \\ 1 + \alpha^r + \beta^r; & \alpha, \beta = \frac{p(p+1)^2}{4} \pm \frac{p(p^2-1)}{12} \sqrt{17}, & q=p^r & \text{[Chandler, Sin and Xiang (2006)].} \end{cases}$$

### 3. Computing $p$ -ranks via the Hilbert Function

Consider the  $[N, k+1]$  code over  $F = \mathbb{F}_q$  spanned by (characteristic vectors of) hyperplanes of  $P^n F$ .

$$q = p^r$$

$$N = \text{number of points} = (q^{n+1} - 1) / (q - 1)$$

$$k = \binom{p+n-1}{n}^r$$

The subcode  $\mathcal{C}$  spanned by complements of hyperplanes has dimension  $k$ .

$\mathcal{V}$ : subset of points of  $P^n F$

$\mathcal{C}_{\mathcal{V}}$ : the code of length  $|\mathcal{V}|$  consisting of *puncturing*:  
restricting  $\mathcal{C}$  to the points of  $\mathcal{V}$

$$\dim(\mathcal{C}_{\mathcal{V}}) = ?$$

### 3. Computing $p$ -ranks via the Hilbert Function

$$F = \mathbb{F}_q$$

$$R = F[X_0, X_1, \dots, X_n] = \bigoplus_{d \geq 0} R_d, \quad R_d = d\text{-homogeneous part of } R$$

Ideal  $I \subseteq R$

$F$ -rational points  $\mathcal{V} = \mathcal{V}(I + J)$ ,  $J = (X_i^q X_j - X_i X_j^q : 0 \leq i < j \leq n)$

$$\mathcal{I} = \mathcal{I}(\mathcal{V}) \subseteq R, \quad \mathcal{I}_d = \mathcal{I} \cap R_d$$

Hilbert Function

$$h_{\mathcal{I}}(d) = \dim(R_d / \mathcal{I}_d)$$

= no. of standard monomials of degree  $d$ ,  
i.e. no. of monomials of degree  $d$  not in  $\text{LM}(\mathcal{I})$

Case  $q=p$ :

$$\dim(\mathcal{C}_{\mathcal{V}}) = h_{\mathcal{I}}(p-1)$$

### 3. Computing $p$ -ranks via the Hilbert Function

$$F = \mathbb{F}_q$$

$$R = F[X_0, X_1, \dots, X_n] = \bigoplus_{d \geq 0} R_d, \quad R_d = d\text{-homogeneous part of } R$$

Ideal  $I \subseteq R$

$F$ -rational points  $\mathcal{V} = \mathcal{V}(I + J)$ ,  $J = (X_i^q X_j - X_i X_j^q : 0 \leq i < j \leq n)$

$$\mathcal{I} = \mathcal{I}(\mathcal{V}) \subseteq R, \quad \mathcal{I}_d = \mathcal{I} \cap R_d$$

*Modified Hilbert Function:*

$h_{\mathcal{I}}^*(d) =$  no. of monomials of

the form  $m_0 m_1^p m_2^{p^2} \dots$

such that  $d = d_0 + p d_1 + p^2 d_2 + \dots$

$\deg(m_j) = d_j$  and  $m_j$  standard

Case  $q = p^r$ : Recall

*Lucas' Theorem.* Write

$$c = c_0 + p c_1 + p^2 c_2 + \dots;$$

$$d = d_0 + p d_1 + p^2 d_2 + \dots$$

Then

$$\binom{d}{c} \equiv \prod_i \binom{d_i}{c_i} \pmod{p}$$

$$\dim(\mathcal{C}_{\mathcal{V}}) = h_{\mathcal{I}}^*(p-1)^r$$

[M. (1997)]

### 3. Computing $p$ -ranks via the Hilbert Function

*Example:* Nondegenerate Quadrics

$I = (Q)$ ,  $Q(X_0, X_1, \dots, X_n) \in R_2$  nondegenerate quadratic form

$F$ -rational points of Quadric

$$Q = \mathcal{V}((Q) + J), \quad J = (X_i^q X_j - X_i X_j^q : 0 \leq i < j \leq n)$$

$\mathcal{C}_Q$  = code over  $F$  of length  $|Q|$  spanned by the  
hyperplane intersections with the quadric

$$\dim(\mathcal{C}_Q) = \left[ \binom{p+n-1}{n} - \binom{p+n-3}{n} \right]^r \quad [\text{Blokhuis and M. (1995)}]$$

### 3. Computing $p$ -ranks via the Hilbert Function

*Example:* Hermitian Variety

$$F = \mathbb{F}_{q^2}, \quad q = p^r$$

$$I = (U), \quad U(X_0, X_1, \dots, X_n) = \sum_i X_i^{q+1} \in R_{q+1}$$

$F$ -rational points

$$\mathcal{H} = \mathcal{V}((U) + J), \quad J = (X_i^{q^2} X_j - X_i X_j^{q^2} : 0 \leq i < j \leq n)$$

$\mathcal{C}_{\mathcal{H}}$  = code over  $F$  of length  $|\mathcal{H}|$  spanned by the hyperplane intersections with  $\mathcal{H}$

$$\dim(\mathcal{C}_{\mathcal{H}}) = \left[ \binom{p+n-1}{n}^2 - \binom{p+n-2}{n}^2 \right]^r \quad [\text{M. (1996)}]$$



### 3. Computing $p$ -ranks via the Hilbert Function

*Example: Grassmann Varieties*

$$F = \mathbb{F}_q, \quad q = p^r$$

Plücker embedding:

$$\left. \begin{array}{l} \text{projective} \\ s\text{-subspaces} \\ \text{of } P^m F \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{points of} \\ P^n F, \quad n = \binom{m+1}{s+1} - 1 \end{array} \right.$$

$I \subseteq R$  generated by homogeneous polynomials of degree 2  
(van der Waerden syzygies)

$F$ -rational points

$$\mathcal{G} = \mathcal{V}(I + J), \quad J = (X_i^q X_j - X_i X_j^q : 0 \leq i < j \leq n)$$

$\mathcal{C}_{\mathcal{G}}$  = code over  $F$  of length  $|\mathcal{G}|$  spanned by the intersections of  
hyperplanes of  $P^n F$  with  $\mathcal{G}$

$$\dim(\mathcal{C}_{\mathcal{G}}) = h_{\mathcal{I}}(p-1)^r, \quad h_{\mathcal{I}}(d) = \prod_{0 \leq j \leq s} \frac{(m+d-s+j)! j!}{(m-s+j)! (d+j)!} \quad [\text{M. (1997)}]$$

### 3. Computing $p$ -ranks via the Hilbert Function

Application:  $F = \mathbb{F}_p$ ,  $\mathcal{O}$  a conic in  $P^2 F$ .

$\mathcal{C}$  = Code of length  $p^2 + p + 1$  spanned by lines

Code spanned by lines		Code spanned by complements of lines
$\mathcal{C}$	$\supset$	$\mathcal{C}^\perp$
dimension $\binom{p+1}{2} + 1$		dimension $\binom{p+1}{2}$

Obtain explicit basis for  $\mathcal{C}^\perp$  using the  $\binom{p+1}{2}$  secants to  $\mathcal{O}$   
and for  $\mathcal{C}$  using the  $\binom{p+1}{2} + 1$  tangents and passants to  $\mathcal{O}$ .

## 4. Open Problems

$$F = \mathbb{F}_q, \quad q = p^r$$

$$N = (q^{n+1} - 1)/(q - 1) = \text{number of points of } P^n F$$

$Q$ : nondegenerate quadric in  $P^n F$

Point-hyperplane  
incidence  
matrix of  $P^n F$ :

	$(P \in Q)$ $P^\perp$	$(P \notin Q)$ $P^\perp$
$P \in Q$		
$P \notin Q$		

$$\text{rank}_F \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array} = \binom{p+n-1}{n}^r + 1$$

$$\text{rank}_F \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array} = \text{rank}_F \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array}$$

$$= \left[ \binom{p+n-1}{n} - \binom{p+n-3}{n} \right]^r + 1$$

$$\text{rank}_F \begin{array}{|c|c|} \hline \square & \square \\ \hline \square & \square \\ \hline \end{array} = ?$$

## 4. Open Problems

$$F = \mathbb{F}_q, \quad q = p^r$$

$Q$ : nondegenerate quadric in  $P^n F$

Can ovoids in  $Q$  exist for  $n > 7$ ?

e.g. for  $n = 23$  we require  $p \geq 59$