Finite Geometry

Zhejiang University, March 2019

A series of talks by Eric Moorhouse, University of Wyoming

I am extremely grateful to Dr. Tao Feng for the opportunity to speak with your research group. I care passionately about my primary research area of finite geometry; and I believe I speak for many of the older practitioners in expressing concerns for the future vitality of our subject. During my 30+ years in finite geometry, I have seen changes in fashionability of work in this area. Many of the big problems seem too hard to offer any realistic hope of progress. Other problems seem to have been overlooked, and are ripe for investigation; but for various reasons, the number of researchers found to work on these problems (which was never particularly large) is probably declining globally. Of course, the same could be rightly said of many other areas of modern mathematics.

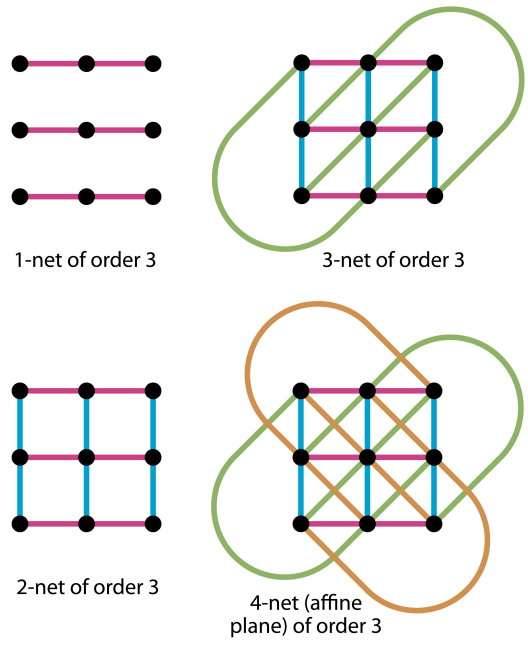
There may be several possible explanations for this state of affairs. In particular, however, I am mindful of how the wider mathematical community has often perceived our subject area, as expressed in Henry Whitehead's words, *"Combinatorics is the slums of topology."* We believe that this image problem is probably changing thanks to the work of such esteemed mathematicians as **Terence Tao**, **Timothy Gowers** and **László Babai**.

My personal goal during my visit, and especially through these talks, is to try to suggest some advice for the future of finite geometry. I am unable to touch on all major themes in finite geometry. I will include almost no proofs of details, and I even omit a bibliography for fears it would be vastly incomplete. Any of these details I can supply if you ask me. However I aim to describe some good problems to work on; and despite the abundance of prohibitively hard problems, I will also include some problems that are both approachable and quite worthwhile. I also hope to describe the current state (and future prospects) for finite geometry, not as an isolated subject, but rather in the context of mainstream mathematics, as I believe that this is imperative for the future of the discipline. In particular, I encourage the next generation of finite geometers to spend some of their time learning methods from analysis, number theory, algebraic geometry, set theory and logic, theoretical computer science, and other areas of mathematics, where much inspiration is to be found for the aspiring finite geometer. In particular, I humbly suggest that methods from classical geometry and infinite settings are not to be avoided; rather they illuminate and clarify many of the difficulties in the finite case, often providing a way forward. Here we hearken to the words of Stanisław Ulam, "The infinite case we shall do right away. The finite may take a little longer."

Lecture 1

Planes, Nets and Webs

For this first lecture, all planes are affine.



(Many of you, however, will no doubt recognize that all our questions may be translated into the language of projective planes.)

A **k-net of order n** has n^2 points, nk lines each with n points, there being k parallel classes of n lines each. Two lines are either parallel or they meet in a unique point. Here it is necessary that $k \leqslant n+1$; and an $(n+1)$-net of order n is an **affine plane**.

All known finite planes have prime power order n. **Gary Ebert** has remarked that "The survival of finite geometry as an active field of study probably depends on someone finding a finite plane of non-prime-power order." This expresses a sentiment (more pessimistic than my own view) about the future of finite geometry. It also articulates what is perhaps the biggest open problem in finite geometry. Because this problem is so difficult, I

prefer to highlight other open problems which I believe offer a more realistic hope for solution.

Participants are presumably aware of the monumental work of **Clement Lam** who, together with several coauthors, showed the nonexistence of a plane of order 10; subsequently also classifying the planes of order 9. The impetus behind this work was supplied by many researchers; but one who deserves particular mention is **John G. Thompson**, best known as a group theorist (at least his Fields Medal was in particular awarded for his earlier work on the odd order paper in group theory). My personal experience, as a doctoral grandchild of Thompson, and as someone who sat through many of his seminars on varied themes, is that the motivation for Thompson's choice of seminar topic of the day would typically be unclear at the beginning of a seminar; but a possible application, to be revealed toward the end of the seminar, was very often the existence question for projective planes of non-prime-power order.

It is my belief that the approach used by Lam et al. for classifying planes of order $n \in \{9, 10\}$ does not scale well for larger values of n. I do, however, believe that other methods are available. In fact I believe that order $n = 11$ (the first case for which uniqueness has not been established) should be easier than order 9 or 10. In general, I believe that prime values of n are easier to deal with than composite.

Take a set of n distinct symbols, $|F| = n$. For a **k-net of order n**, we label points by a subset $\mathcal{N} \subseteq F^k$. We also index the n lines of each parallel class using the elements of F. A typical point $(a_1, a_2, \ldots, a_k) \in \mathcal{N}$ lies on line a_i of the i-th parallel class. We may assume $(0, 0, \ldots, 0) \in \mathcal{N}$. This coordinate description of a net captures completely what a net is about. That is, an equivalent definition of a k-net of order n is: a subset $\mathcal{N} \subseteq F^k$ consisting of $|\mathcal{N}| = n^2$ vectors $(a_1, a_2, \ldots, a_k) \in \mathcal{N}$, each of which is uniquely determined by any two of its coordinates.

Unless otherwise indicated, I will take $F = \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ where p is prime. Now the **classical affine plane of order p** has the coordinate description

$$\mathcal{N} = \{(x,\ y,\ x+y,\ 2x+y,\ \ldots,\ (p-1)x+y)\ :\ x, y \in F\}.$$

The major open problem which motivates our investigation is: Must every plane of prime order p be classical?

Let $\mathcal{N}$ be a k-net of prime order p. The set of all k-tuples $(f_1, f_2, \ldots, f_k)$ of functions $f_i : F \to F$ such that $f_i(0) = 0$ and

$$f_1(a_1) + f_2(a_2) + \cdots + f_k(a_k) = 0$$

for all $(a_1, a_2, \ldots, a_k) \in \mathcal{N}$, forms a vector space $\mathcal{V} = \mathcal{V}(\mathcal{N})$.

For example, consider the classical 4-net

$$\mathcal{N} = \{(x,\ y,\ x+y, x+\alpha y)\ :\ x, y \in F\}$$

where $\alpha \neq 0, 1$. Here the space $\mathcal{V}$ consists of all 4-tuples (f_1, f_2, f_3, f_4) of functions $F \to F$ of the form

$$\begin{aligned} f_1(t) &= (a+b)t + (1-\alpha)ct^2, \\ f_2(t) &= (a+\alpha b)t + (\alpha-1)\alpha ct^2, \\ f_3(t) &= -at + \alpha ct^2, \\ f_4(t) &= -bt - ct^2 \end{aligned}$$

for some $a, b, c \in F$, so $\dim \mathcal{V} = 3$.

Conjecture. *For any k-net of prime order p,*

$$\dim \mathcal{V}(\mathcal{N}_k) \leqslant \tfrac{1}{2}(k-1)(k-2).$$

Moreover for any sequence of subnets $\mathcal{N}_1 \subset \mathcal{N}_2 \subset \cdots \subset \mathcal{N}_k$,

$$\dim \mathcal{V}(\mathcal{N}_{i+1}) - \dim \mathcal{V}(\mathcal{N}_i) \leqslant i - 1.$$

If this conjecture holds, then all planes of prime order are classical!

Plane curves of degree k have genus $g \leqslant \frac{1}{2}(k-1)(k-2)$. This bound is not a coincidence—I will say a little about the connection below.

Theorem. *For 3-nets of prime order p, the conjectured bound $\dim \mathcal{V}(\mathcal{N}_3) \leqslant 1$ holds. We have equality iff the net is cyclic (i.e. a subnet of a classical plane).*

Proof. $\mathcal{N}$ is a set of p^2 triples $(x, y, z) \in F^3$, $F = \mathbb{F}_p$, such that any triple is uniquely determined by two of its coordinates. Let $(f, g, h) \in \mathcal{V}(\mathcal{N})$, so $f(0) = g(0) = h(0) = 0$ and

$$f(x) + g(y) + h(z) = 0 \quad \text{for all } (x, y, z) \in \mathcal{N}.$$

Let $\zeta = e^{2\pi i/p}$ and consider the exponential sum $S_f = \sum_{x \in F} \zeta^{f(x)}$. Then

$$S_f S_g = \sum_{x,y \in F} \zeta^{f(x)+g(y)} = p \sum_{z \in F} \zeta^{-h(z)} = p\overline{S_h}.$$

We get

$$S_f S_g S_h = p S_h \overline{S_h} = p|S_h|^2.$$

By symmetry, $|S_f| = |S_g| = |S_h| \in \{0, p\}$.

If $|S_f| = |S_g| = |S_h| = p$ then f, g, h are constant functions. However, $f(0) = g(0) = h(0) = 0$ so $f = g = h = 0$.

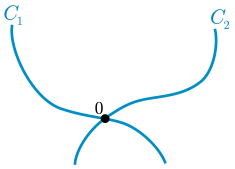
Otherwise $S_f = S_g = S_h = 0$ so f, g, h are permutations of F. After relabelling if necessary, we may

assume $f(x) = x$, $g(y) = y$ and $h(z) = z$. Since $z = h(z) = -f(x)-g(y) = -x-y$ we get a cyclic 3-net

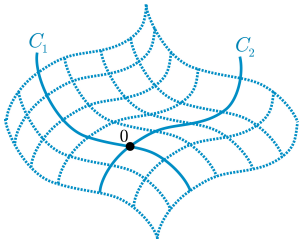
$$\mathcal{N} = \{(x, y, -x-y) : x, y \in F\}. \qquad \square$$

The analogue of the conjecture for webs (e.g. over $\mathbb{R}$ or $\mathbb{C}$) is actually a theorem. This connection dates back to the earliest papers of **Sophus Lie**, who introduced double translation surfaces (defined below), these being equivalent to 4-webs. (Lie was led to this through his work on minimal surfaces.) **Henri Poincaré** gave an alternative treatment of these results, replacing Lie's methods (primarily brute force) by an application of the theorem of **Niels Abel** regarding differentials on an algebraic curve. This connection was further pursued in papers of **Phillip Griffiths** and **Shiing-Shen Chern**. Indeed, Chern's doctoral work was on the subject of webs; and during his later career, he was known to refer to web theory as his favourite mathematics. **Bernard Saint-Donat**, a student of **David Mumford**, became interested in extensions of this work to prime characteristic; and his student **John Little** (of Cox-Little-O'Shea) published some versions for webs over $F = \mathbb{Q}_p$ or $\mathbb{F}_p(t)$ (in place of $\mathbb{R}$ and $\mathbb{C}$).

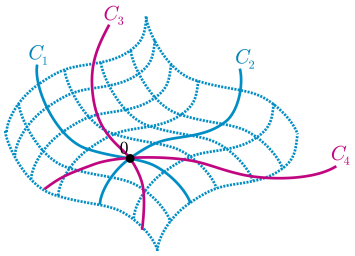
Let C_1 and C_2 be two smooth curves passing through the origin in $\mathbb{R}^d$, intersecting transversely (i.e. not having a common tangent line).



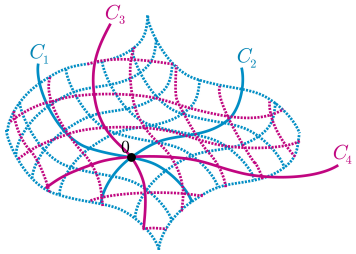
The **Minkowski sum** C_1+C_2 is the surface consisting of all points $u_1+u_2 \in \mathbb{R}^d$ where $u_i \in C_i$.



Suppose curves C_3 and C_4 also lie in this same surface, such that each pair of curves C_i and C_j intersects transversely at the origin.



If it happens that $C_3+C_4 = C_1+C_2$ (a very strong condition), then this surface is called a **double translation surface**.



Theorem [Lie]**.** *Any double translation surface in $\mathbb{R}^d$ must lie in a subspace of dimension at most 3. When the surface spans $\mathbb{R}^3$, the tangent lines to the curves C_i meet the plane at infinity in a curve C of degree 4 and genus 3; and the surface may be recovered from C.*

Example 1 (Lie). Fix $\alpha \notin \{0, 1\}$. The quadric $z = \alpha x^2 - y^2$ in $\mathbb{R}^3$ is a double translation surface $C_1+C_2 = C_3+C_4$ where

$$\begin{aligned} C_1 &= \{(s, 0, \alpha s^2) \,:\, s \in \mathbb{R}\}; \\ C_2 &= \{(0, t, -t^2) \,:\, t \in \mathbb{R}\}; \\ C_3 &= \{(u, \alpha u, \alpha(1-\alpha)u^2) \,:\, u \in \mathbb{R}\}; \\ C_4 &= \{(v, v, (\alpha-1)v^2) \,:\, v \in \mathbb{R}\}. \end{aligned}$$

In this case the curve C at infinity is a singular curve of degree four with equation $XY(X-Y)(\alpha X-Y) = 0$.

Example 2 (Lie). Fix $\alpha \notin \{0, \frac{1}{2}\}$. The transcendental surface

$$z = (x+1)e^{-2\alpha y} - 1 + \alpha x(x+2)$$

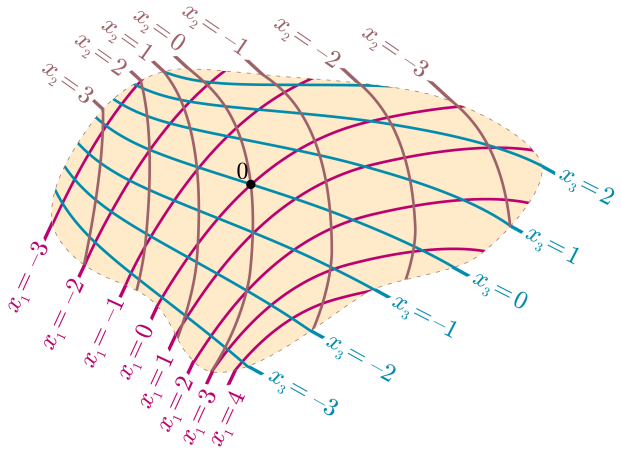
in $\mathbb{R}^3$ is a double translation surface $C_1+C_2 = C_3+C_4$ where

$$\begin{aligned} C_1 &= \{(s, 0, \alpha s^2+(2\alpha+1)s) \,:\, s \in \mathbb{R}\}; \\ C_2 &= \{(\tfrac{1}{2\alpha}(1-e^{-2\alpha t}), t, \tfrac{1}{4\alpha}(1-e^{-4\alpha t})) \,:\, t \in \mathbb{R}\}; \\ C_3 &= \{(0, u, e^{-2\alpha u}-1) \,:\, u \in \mathbb{R}\}; \\ C_4 &= \{(v, \tfrac{1}{2\alpha}\ln(1+v), \alpha v(v+2)) \,:\, v > -1\}. \end{aligned}$$

In this case the curve C at infinity is a singular curve of degree four with equation $XY(X^2-YZ) = 0$.

A **(2-dimensional) k-web** has point set $\mathcal{W} \subset \mathbb{R}^2$, an open neighbourhood of $\mathbf{0}$. It has k smooth coordinate functions $x_1, x_2, \ldots, x_k : \mathcal{W} \to \mathbb{R}$ such that for all $i \neq j$,

∇x_i and ∇x_j are linearly independent throughout $\mathcal{W}$; also $x_i(\mathbf{0}) = 0$.



A 3-web

The level curves for $x_1, x_2, \ldots, x_k$ intersect transversely, forming the 'lines' of the web. Point $P \in \mathcal{W}$ has k coordinates $x_1(P), x_2(P), \ldots, x_k(P)$, any two of which uniquely determine the point P. Two webs *are the same* if they agree in a neighbourhood of $\mathbf{0}$ (so only the germs of the coordinate functions x_i are relevant).

Consider the vector space $\mathcal{V}$ consisting of all k-tuples $(f_1, f_2, \ldots, f_k)$ of smooth functions $f_i : \mathbb{R} \to \mathbb{R}$ such that $f_i(0) = 0$ and

$$f_1(x_1(P)) + \cdots + f_k(x_k(P)) = 0$$

for all $P \in \mathcal{W}$.

The **rank** of $\mathcal{W}$ is $\dim \mathcal{V} \leqslant \frac{1}{2}(k-1)(k-2)$. Equality is attained for **algebraic k-webs** obtained from plane curves of degree k having maximal genus (so-called **extremal** curves). For $k \geqslant 5$, other examples are known.

Lecture 2

Planes and their Substructures

In this talk, all planes considered are *projective*.

Every field F gives rise to a **classical projective plane** $\mathbb{P}^2F$ whose points and lines are the one- and two-dimensional subspaces of F^3.

A **projective plane of order** $n \geqslant 2$ has n^2+n+1 points and n^2+n+1 lines. Each line has $n+1$ points, and each point is on $n+1$ lines. Any two points lie on exactly one common line. Any two distinct lines meet in exactly one point.

The finite classical plane $\mathbb{P}^2\mathbb{F}_q$ has prime power order q. And there exist finite non-classical planes, but in all known cases, their order is a prime power. The only known planes of prime order are the classical ones $\mathbb{P}^2\mathbb{F}_p$.

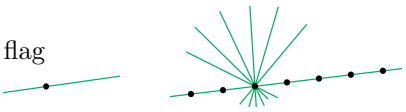
A **partial linear space (PLS)** is an incidence system of points and lines in which no two distinct points are joined by more than one line, i.e.  *does not* occur. (Some authors require every line to have at least two points. Connectedness is never required.)

The point-line dual of a partial linear space (in which we reverse the roles of points and lines) is a partial linear space. The **incidence graph** of a PLS is a bipartite graph of girth at least 6 (i.e. no 4-cycles).

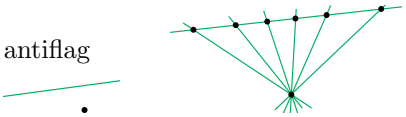
A **linear space** is a PLS in which any two points are joined by a (necessarily unique) line.

If a linear space is also a dual linear space (i.e. any two lines intersect), then either

- it contains a **quadrangle** (four points, no three collinear). In this case the space is a projective plane. *Or*
- It does not contain a quadrangle. In this case it is a **generalized flag** or a **generalized antiflag**.



generalized flag

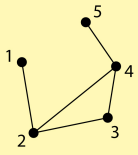


generalized antiflag

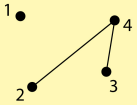
It is to be understood that some more trivial substructures (such as the empty configuration) must be included in our list, by viewing them as special cases of generalized flags or antiflags. The triangle may be viewed either as a generalized antiflag, or as the projective plane of order 1. Note that a generalized flag (or antiflag) may have differing numbers of points and lines. Substructures arise naturally as fixed point substructures of collineations (automorphisms) although in the finite case, fixed substructures of collineations have equally many points and lines. This is no longer true in the infinite case, a point which we will visit in the next lecture.

As in graph theory, where one must distinguish between subgraphs and induced subgraphs of a graph, a

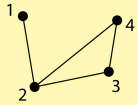
comparable distinction arises in the theory of partial linear spaces. Recall that given a graph Γ with vertex set V, an **induced subgraph** of Γ has vertex set $V' \subseteq V$. Its edges are all edges of Γ joining vertices in V'. A **subgraph** of Γ has vertex set $V' \subseteq V$, and edges given by a *subset* of the edges in Γ joining vertices in V'.



a graph Γ



a *subgraph* of Γ (*not* induced)



the subgraph of Γ *induced* on {1,2,3,4}

Let $(\mathcal{P}, \mathcal{L}, I)$ be a partial linear space (with point set $\mathcal{P}$, line set $\mathcal{L}$ and incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$). Any subsets of the points and lines $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$ give rise to an **induced substructure** $(\mathcal{P}', \mathcal{L}', I \cap (\mathcal{P}' \times \mathcal{L}'))$. Starting from the incidence graph of $(\mathcal{P}, \mathcal{L}, I)$, here one takes the *induced subgraph* on the vertices $\mathcal{P}' \cup \mathcal{L}'$.

If instead $I' \subseteq I \cap (\mathcal{P}' \times \mathcal{L}')$, then $(\mathcal{P}', \mathcal{L}', I')$ is a **substructure** of $(\mathcal{P}, \mathcal{L}, I)$. Here one takes simply a *subgraph* of the incidence graph.

An **embedding** of one PLS $(\mathcal{P}, \mathcal{L}, I)$ in another, $(\widehat{\mathcal{P}}, \widehat{\mathcal{L}}, \widehat{I})$, is a pair of injections $\iota : \mathcal{P} \to \widehat{\mathcal{P}}$, $\mathcal{L} \to \widehat{\mathcal{L}}$ such that $(P, \ell) \in I \Rightarrow (\iota(P), \iota(\ell)) \in \widehat{I}$. The embedding is **strict** if $(P, \ell) \in I \Leftrightarrow (\iota(P), \iota(\ell)) \in \widehat{I}$. The image of an embedding is a substructure, whereas the image of a strict embedding is an induced substructure. *Every* embedding of a linear space is strict.

Examples of embeddings: $\mathbb{A}^2\mathbb{F}_3 =$  embeds in $\mathbb{P}^2F$ iff $\mathrm{char}(F) = 3$ or F has a primitive cube root of unity. (Note: $\mathbb{F}_q$ satisfies this condition iff $q \not\equiv 2 \bmod 3$.)

The Desargues configuration  (10 points, 10 lines) embeds in every finite projective plane of order $q > 2$ (strongly, for $q > 3$).

The projective plane of order two $\mathbb{P}^2\mathbb{F}_2 =$  embeds in most known finite planes. **Neumann's Conjecture** states that the only finite projective planes without a subplane of order two are the classical planes of odd order. The projective plane of order three $\mathbb{P}^3\mathbb{F}_3$ embeds in many (yet a small percentage) of known finite planes.

Every PLS embeds in an infinite projective plane (by a process of free closure).

Open Question [Erdős 1979 and probably earlier]. Must every finite PLS embed in a *finite* projective plane?

(It is equivalent to consider only linear spaces, so any embedding is strict.) Expert opinion/intuition is quite mixed regarding the answer to this question.

We know that there exist finite PLS's which do not embed in Hughes planes or André planes (a particular class of translation planes), but no finite PLS is known to not embed in any finite translation plane, even if one restricts to 'two-dimensional translation planes' (i.e. arising from line spreads of $\mathbb{P}^3\mathbb{F}_q$).

If one relaxes 'spread' to 'partial spread', then we are in much better shape (although the harder problem then becomes trying to extend the partial spread to a spread):

Theorem [M. and Williford, 2009]**.**

(i) Every finite PLS is embeddable in a finite translation net generated by a partial spread of a finite vector space.

(ii) Let p be prime and let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. Then every finite PLS is embeddable in a translation plane of finite dimension over $\overline{\mathbb{F}_p}$.

Unfortunately in (ii), the embedding is not known to lie in a finite subplane (despite the fact that every finite subset of $\overline{\mathbb{F}_p}$ lies in a finite subfield).

Finite geometry currently suffers from a lack of any thorough investigation of the complexity of basic computational tasks, comparable to what is now available in graph theory and in much of algebra (particularly group theory)!

Given two finite planes Π and $\widetilde{\Pi}$ of order $< n$, one can answer the question 'Does Π embed in $\widetilde{\Pi}$?' in time bounded by a polynomial in n. But if Π is replaced by a more general finite PLS, *this is probably not true . . . even if $\widetilde{\Pi}$ is a classical plane!*

Lower Bounds on Complexity of Embedding a PLS:

Given n, choose M to be a random n-bit integer, so $n = O(\log M)$. We have shown how to construct a partial linear space $\Pi(M)$ of size $O(n)$, such that in order to *construct* an embedding $\Pi(M) \hookrightarrow \mathbb{P}^2\mathbb{F}_q$ for some q, requires first factoring M. The best known algorithms for this have subexponential execution time $O(exp(cn^{1/3} \log^{2/3} n))$.

It may be possible to nonconstructively prove embeddability without producing such an embedding, but we do not know how. Our best algorithm for solving the embedding problem, requires non-polynomial (in fact subexponential) time.

Upper Bounds on Complexity of Embedding a PLS:

Let Π be a partial linear space of size $O(n)$, and let p be prime. Then Π embeds in $\mathbb{P}^2\mathbb{F}_{p^e}$ for some $e \geqslant 1$,

iff Π embeds in $\mathbb{P}^2\overline{\mathbb{F}_p}$ where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$.

In general the best way I know how to decide existence of such an embedding, is to solve a system of polynomial equations by existing methods from computational commutative algebra. Known methods, however, are practical only for small n; both the space and time requirements are exponential ($O(exp(n^4))$ for deterministic algorithms, $O(exp(n^2))$ for nondeterministic algorithms).

Perhaps worst of all, we see no evidence that the embedding question is in NP (although for *fixed* p, it seems that deciding embeddability in characteristic p is in co-NP).

Let Π be a finite PLS. I believe that the question of embeddability of Π in a finite classical plane is hard to determine. So I believe that the question of embeddability of Π in an arbitrary finite classical plane, must be *extremely* hard.

More Open Questions

Q: Must every finite plane of order n^2 have a subplane of order n? (And a unital of order n?)

Q: Must every finite plane Π have a proper extension (i.e. does Π embed in a larger finite plane)?

In $\mathbb{P}^2\mathbb{F}_{p^e}$, every quadrangle generates a subplane of order p. Gleason's theorem shows that if any quadrangle in Π generates a subplane of order 2, then $\Pi \cong \mathbb{P}^2\mathbb{F}_{2^e}$.

Q: Are there any primes other than 2 for which the corresponding statement holds?

Q: If Π is a finite plane for which every quadrangle generates a *proper* subplane, must Π be classical (of order p^e, $e \geqslant 2$)?

Q: Can a plane of order $n > 3$ embed in a plane of order *not* a power of n?

Number theory abounds in hard problems for which *conjectural* answers can be deduced using certain *heuristics*. Finite geometry needs more heuristics like this:

Let k be a small positive integer. Given a plane Π, let $N_k(\Pi)$ be the number of subplanes of order k. Heuristically, if Π has order $n \gg 2$, then

$$N_2(\Pi) \approx \tfrac{1}{168} n^3(n^3-1)(n+1) \sim \tfrac{1}{168} n^7.$$

This heuristic applies best to the 'uglier' planes (those with very few automorphisms). For example:

For planes of order 25, the heuristic says $N_2(\Pi) \approx$ **37,781,250**. There are 193 planes of order 25 known; and ignoring the classical and Hughes planes, the number of subplanes of order 2 varies from

35,110,000 to **43,569,000**.

The results for planes of order 49 are *much* better.

Similar counts for larger fixed k leads to

$$N_k(\Pi) \approx c_k n^{(3-k)(k^2+k+1)}$$

as $n \to \infty$, where c_k is a positive constant depending only on k. For example, $N_3(\Pi) = O(1)$ and $N_4(\Pi) = O(n^{-21})$.

Among the hundreds of thousands of known planes of order 49, about 1 in every 20,000 has subplanes of order 3; and no subplanes of order 4 have been found.

As $n \to \infty$, the hope of finding subplanes of order 4 seems to *decrease*, contrary to some expectations.

Tim Penttila has widely circulated the following scheme for finding a plane of non-prime-power order: Start with a known plane Π of *large* order n. Sample quadrangles at random and look at what subplanes they generate. My assertion is that you won't find any subplanes of order other than 2 this way. Tim doesn't believe my heuristics.

Lecture 3

Geometry Beyond the Finite

Let $(\mathcal{P}, \mathcal{L}, I)$ be a partial linear space.

A **partial spread** is a collection of mutually disjoint lines $\Sigma \subseteq \mathcal{L}$, i.e. no two lines in Σ intersect. A **spread** is a partial spread covering the points, i.e. $\bigcup \Sigma = \mathcal{P}$. Equivalently, a spread is a partition of the points into lines.

Projective 3-space over a field F is denoted $\mathbb{P}^3F$. It has points, lines and planes given by the subspaces of F^4 of dimension 1, 2 and 3.

In the finite case, $\mathbb{P}^3\mathbb{F}_q$ has $(q^2+1)(q+1)$ points, and each line has $q+1$ points. So every partial spread has at most q^2+1 lines. A spread is the same thing as a set of q^2+1 mutually disjoint lines. Every such spread gives a plane of order q^2, known as a **translation plane**. Take F^4 as points, and the *cosets* of the q^2+1 subspaces $\ell \in \Sigma$ as lines, to get an affine plane of order q^2; and this gives the affine translation plane arising from Σ.

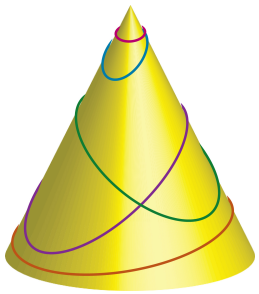
The biggest obstacle to constructing spreads (and hence translation planes) is the fact that not every partial spread can be extended to a spread. But the infinite case is much easier:

Let F be an infinite field. Then every partial spread of $\mathbb{P}^3F$ having fewer than $|F|$ lines, can be extended to a spread, by a process of transfinite induction.

(In order to get a translation plane, we need the spread to also be a dual spread: every plane of $\mathbb{P}^3F$ should contain a line of the spread. But this is easily arranged. In the finite case every spread is also a dual spread, by the pigeonhole principle, so this issue doesn't even arise.)

So we get a *huge variety* of translation planes in the infinite case, practically for free.

I have used a similar idea to extend a partial flock to a flock of a quadratic cone, answering a question posed by Norman Johnson at the 1996 conference *Mostly Finite Geometries*.



A **flock** of a quadratic cone is a partition of its $q(q+1)$ points (minus the vertex) into q conics of size $q+1$.

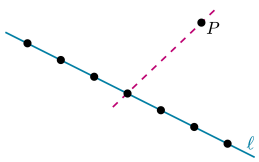
A **collineation** of a projective plane Π is a bijection of its points, which also gives a bijection on the lines. An automorphism of the bipartite incidence graph is either a *collineation* (mapping points $\to$ points, and lines $\to$ lines) or a **correlation** (interchanging points $\leftrightarrow$ lines).

The group of all collineations of Π is denoted $\mathrm{Aut}\,\Pi$.

Let Π be a projective plane. In the finite case, $\mathrm{Aut}\,\Pi$ has equally many orbits on points and on lines. (The same conclusion holds for automorphisms of symmetric designs, character tables of finite groups, etc.)

Does the same conclusion hold for infinite projective planes Π? Cameron (1991) posed this question, which he attributed to Kantor. We found a negative answer to this question:

Theorem [M. and Penttila, 2014]. *Let A and B be any two nonzero cardinal numbers. Then there is a projective plane whose collineation group has A orbits on points and B orbits on lines.*



A **GQ (generalized quadrangle) of order** (s,t) has

- $s+1$ points on every line; $t+1$ lines through every point; and
- if point P is not on line ℓ, then there is a unique line through P meeting ℓ.

We generally require $s,t>1$.

In the finite case ($s,t<\infty$): There are $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines. Also $\sqrt{t}\leqslant s\leqslant t^2$, i.e. $\sqrt{s}\leqslant t\leqslant s^2$.

Q: Can one of s,t be finite and the other infinite?

That is, we suppose a GQ has finite linesize $s+1<\infty$. Must the GQ be finite (i.e. is $t<\infty$)?

A GQ with **three** points per line is finite. (Elementary proof, one short paragraph; Cameron)

A GQ with **four** points per line is finite. (Four-page paper; Brouwer 1991)

A GQ with **five** points per line is finite. (Cherlin 2005 using mathematical logic)

Line size **six** (and higher) is completely open!

Mathematical logic supplies methods for *constructing examples* but also for *proving nonexistence*.

Orbits on k-tuples of points

Consider the classical projective plane $\Pi=\mathbb{P}^2F$ over a field F. The collineation group $\mathrm{Aut}\,\Pi$ permutes points transitively (i.e. just one orbit on points).

There are two orbits on ordered pairs of points: (P,P), (P,Q), $P\neq Q$.

There are six orbits on ordered triples of points: (P,P,P), (P,P,Q), (P,Q,P), (Q,P,P), (P,Q,R) collinear, (P,Q,R) noncollinear where P,Q,R are distinct.

If F is infinite, there are *infinitely many orbits* on 4-tuples of points. (For four collinear points, the cross ratio has infinitely many possible values.)

Let Π be a (countably) infinite plane. Suppose that for every $k\geqslant 1$, $\mathrm{Aut}\,\Pi$ has only *finitely many orbits* on k-tuples of points. (One could say instead k-sets of points, or k-sets of lines, etc. and this condition is unchanged.) Then we say Π is **$\aleph_0$-categorical**. (This is not the actual definition of $\aleph_0$-categoricity; but it gives an honest example, without sacrificing anything from the original problem.)

Open Problem. *Does there exist an $\aleph_0$-categorical plane?*

As we have indicated, an $\aleph_0$-categorical plane *cannot be classical*. If there exists an $\aleph_0$-categorical plane, it would have a *much* bigger group of automorphisms than any classical plane. Here 'bigger' refers to the much higher degree of transitivity on substructures; but also cardinality—countable classical planes have countably infinite collineation groups, whereas the collineation group of an $\aleph_0$-categorical plane would have cardinality $2^{\aleph_0}$. This *seems* inconceivable.

Suppose Π is an $\aleph_0$-categorical projective plane. We try to get a contradiction.

Lemma. *Any finite list of points $P_1, P_2, \ldots, P_r$ which includes a quadrangle, must generate a finite subplane.*

Proof. Starting with $\mathcal{P}_1 = \{P_1, P_2, \ldots, P_r\}$ and alternately joining points and intersecting lines, we get a sequence of substructures with point sets

$$\mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \mathcal{P}_3 \subseteq \cdots$$

whose union gives a subplane $\mathcal{P}_\infty = \bigcup_i \mathcal{P}_i \subseteq \Pi$.

If this sequence is *strictly increasing*, choose points $T_i \in \mathcal{P}_{i+1} \setminus \mathcal{P}_i$; then the $(r+1)$-tuples $(P_1, P_2, \ldots, P_r, T_i)$ $(i \geqslant 1)$ are in distinct orbits, a contradiction. So we must have $\mathcal{P}_i = \mathcal{P}_\infty$ for all sufficiently large i. □

Now let (P_i, Q_i, R_i, S_i) $(i = 1, 2, \ldots, m)$ be representatives of the orbits of $\mathrm{Aut}\,\Pi$ on quadrangles. If n_i is the order of the subplane generated by P_i, Q_i, R_i, S_i, then *every quadrangle* generates a subplane of order at most

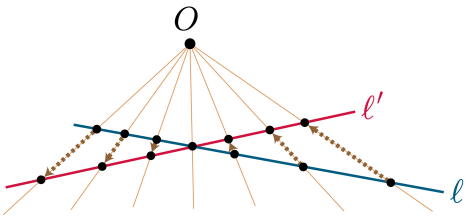
$$n = \max\{n_1, n_2, \ldots, n_m\}.$$

Let $\Pi_0 \subset \Pi$ be any finite subplane of order $> n$. (This is easily found; for example any quadrangle, together with any $n+2$ collinear points, will together generate such a subplane.) Note that every quadrangle in Π_0 generates a proper subplane.

Without loss of generality, Π_0 is non-classical. (As we have observed, Π itself is non-classical. So there exists an induced substructure in Π violating Desargues' Theorem. Without loss of generality, Π_0 was chosen so as to contain this substructure.)

So if there exists an $\aleph_0$-categorical plane, then we obtain *many* examples of finite nonclassical planes in which every quadrangle generates a proper subplane. Such a conclusion seems highly improbable, although we have not yet found a contradiction.

Now fix lines $\ell \neq \ell'$ in a projective plane Π. Each point $O \notin \ell \cup \ell'$ determines a bijection from the points of ℓ to the points of ℓ', called a **perspectivity**.



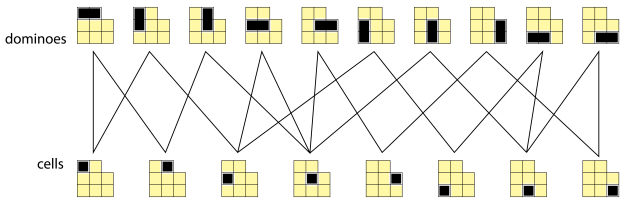
Compositions of perspectivities gives the **projectivity groupoid of Π**. In particular for each line ℓ, we get a group of permutations of the points of ℓ, called the **projectivity group** of Π. This group doesn't really depend on the choice of line ℓ.

A classical plane $\Pi = \mathbb{P}^2 F$ has collineation group $\mathrm{Aut}\,\Pi \cong P\Gamma L_3(F)$ and projectivity group $PGL_2(F)$. A finite nonclassical plane Π of order n has typically *small* collineation group $\mathrm{Aut}\,\Pi$, but *very large* projectivity group A_{n+1} or S_{n+1}. An $\aleph_0$-categorical plane would have collineation group of order $2^{\aleph_0}$ but projectivity group of order $\aleph_0$.

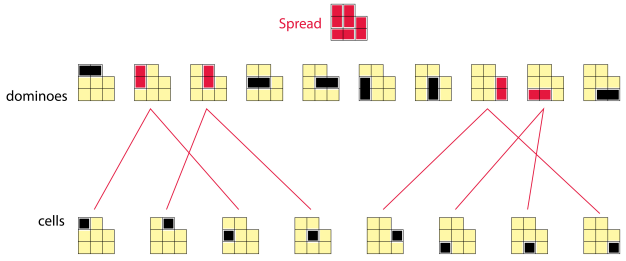
Lecture 4

Ovoids and Spreads

Consider a bipartite graph representing incidences between *points* and *blocks*.

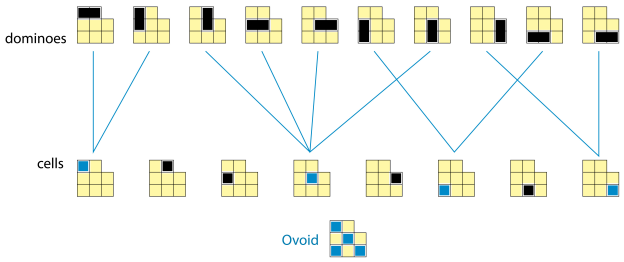


A **spread** is a set of blocks partitioning the points:

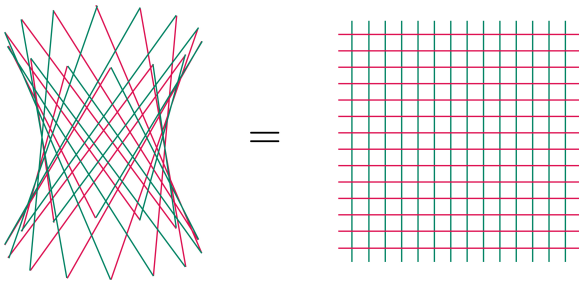


Dually, an **ovoid** is a set of points partitioning the

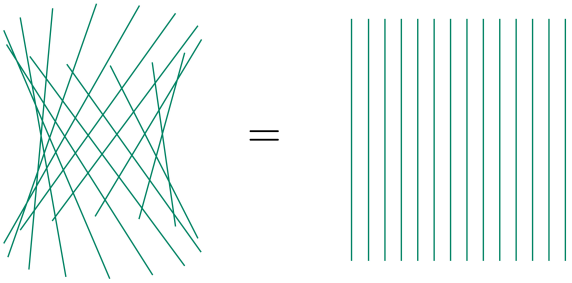
blocks:



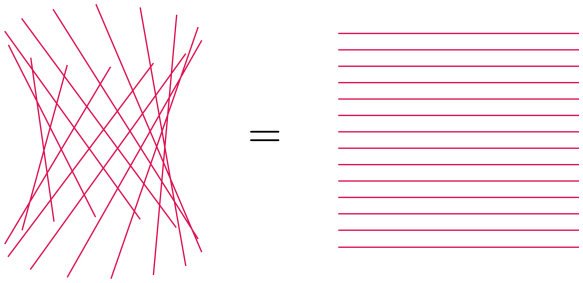
A basic example of such a point-block incidence system is a **hyperbolic quadric** in projective 3-space $\mathbb{P}^3\mathbb{F}_q$. This is a ruled quadric: combinatorially it is just a $(q+1) \times (q+1)$ grid. It has $(q+1)^2$ points and $2(q+1)$ lines.



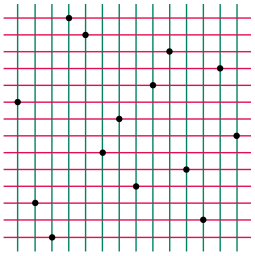
This quadric has exactly two spreads. One is



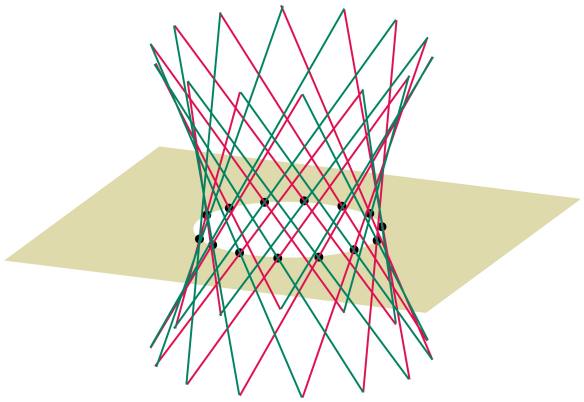
and the other is



There are $(q+1)!$ *ovoids* (transversals of the grid), e.g.:



This includes $q(q^2-1)$ **regular ovoids**, which are nonsingular plane sections of the quadric:



Some ovoids in the Klein quadric in $\mathbb{P}^5\mathbb{F}_p$

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

- $x_i \equiv 1 \bmod 4$; and
- $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

Example $[p = 5,\ |\mathcal{S}| = 5^2 + 1 = 26]$

$\mathcal{S}$ contains 6 vectors of shape $(5, 1, 1, 1, 1, 1)$;
20 vectors of shape $(-3, -3, -3, 1, 1, 1)$.

Example $[p = 13,\ |\mathcal{S}| = 13^2 + 1 = 170]$

$\mathcal{S}$ contains 20 vectors of shape $(5, 5, 5, 1, 1, 1)$;
30 vectors of shape $(-7, -5, 1, 1, 1, 1)$;
60 vectors of shape $(5, 5, -3, -3, -3, 1)$;
60 vectors of shape $(-7, -3, -3, -3, 1, 1)$.

Points of $\mathbb{P}^5\mathbb{F}_p$ satisfying $\sum_i x_i^2 = 0$ form the **Klein quadric** with $(p^2+1)(p^2+p+1)$ points and $2(p^2+1)(p+1)$ planes. Each point is in $2(p+1)$ planes, so an *ovoid* is any set of p^2+1 points, no two on the same plane (no two perpendicular). This is the same thing as a spread of lines in $\mathbb{P}^3\mathbb{F}_p$, i.e. a partition of the $(p^2+1)(p+1)$ points into p^2+1 lines (of size $p+1$). And this is the same thing as a *translation plane* of order p^2.

S_6-invariant ovoids in the Klein quadric

Now let $F = \mathbb{F}_q$, $q \equiv 1 \bmod 4$. The vectors in F^6 satisfying $\sum_i x_i^2 = 0$ form (projectively) a Klein quadric.

When can we find an ovoid in the quadric invariant under S_6 acting by coordinate permutations? (We need

q^2+1 vectors satisfying $x \cdot y = 0$ iff $x = y$. And we want the set to be invariant under coordinate permutations.)

Q: Must q be prime?

Usually when a combinatorial problem has a solution over $\mathbb{F}_p$, the solution generalizes to $\mathbb{F}_q$, $q = p^e$. The situation above seems to be an example to the contrary.

Let $F = \mathbb{F}_q$ where q is an odd prime. The **triality quadric** in $\mathbb{P}^7 F$ with equation $\sum_i x_i^2 = 0$ contains

- $(q^3+1)(q^2+1)(q+1)$ points;
- $2(q^3+1)(q^2+1)(q+1)$ solids, i.e. projective 3-spaces, the maximum dimension of any subspaces lying in the quadric; and
- $2(q^2+1)(q+1)$ solids containing each point.

So an *ovoid* (set of points hitting each solid exactly once) must have size q^3+1. Note, by the way, that the number of points on the quadric is divisible by q^3+1; so it seems reasonable to ask whether the quadric can be partitioned into ovoids. Such a partition, if it exists, has been called a **fan**, although there is scarce literature on the notion.

We now ask: do ovoids *exist* in the triality quadric? There is a very prolific source of ovoids which we proceed to describe.

The E_8 Root Lattice

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z},\ x_1 \equiv x_2 \equiv \cdots \equiv x_8 \bmod 2, \text{ and } \sum_i x_i \equiv 0 \bmod 4.$$

This is the E_8 **root lattice**. It is

- a **lattice** (i.e. additive subgroup of $\mathbb{R}^8$);
- **integral** ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- **unimodular** (its density is 1, i.e. it has one point per unit volume on average);
- it has **minimum distance** $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

E has 240 shortest vectors ($e \in E$, $\|e\|^2 = e \cdot e = 2$) called **root vectors**:

- $(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0)$ and permutations thereof (112 vectors of this shape); and
- $\frac{1}{2}(\pm 1, \pm 1, \ldots, \pm 1)$ with an even number of '$-$' signs (128 vectors of this shape).

For an odd prime p, there are $240(p^3+1)$ vectors $x \in E$ with $\|x\|^2 = 2p$.

Theorem [Conway et. al., 1988]**.** *For every prime p, there is an ovoid in the triality quadric in $\mathbb{P}^7\mathbb{F}_p$.*

Idea of proof: Take p to be an *odd* prime (the case $p = 2$ was previously solved. Fix a root vector $e \in E$.

Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v = e + 2x$ for some $x \in E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. □

Using E, Conway et. al. gave more examples of ovoids in the triality quadric (up to 3 examples for each prime p). Also using E, we (1993) generalized this to an unbounded number of examples for each p. Other constructions of ovoids in the triality quadric are known, but *almost all of them come from the E_8 root lattice.*

It is really this construction of ovoids from E_8, which explains the earlier examples of ovoids in the Klein quadric (and *many* similar examples).

The geometry of the triality quadric admits a triality automorphism, mapping ovoids to spreads.

Open Questions

Q: Do ovoids exist in the triality quadric in $\mathbb{P}^7\mathbb{F}_q$ for every q? The smallest open case is $q = 25$.

Q: Is it true that the number of ovoids in the triality quadric is unbounded as $p \to \infty$?

Q: If an ovoid in the triality quadric admits certain groups (such as $Sp_6(\mathbb{F}_q)$), must it come from the E_8 construction, with $q = p$?

Q: Construct an ovoid in the triality quadric admitting no automorphisms (a 'rigid' ovoid).

Q: Prove that for the triality quadric in $\mathbb{P}^7\mathbb{F}_p$ arising from E_8, the total number of ovoids arising from E_8 is $\frac{|G(p)|}{4|G(2)|}(p^4 + 239)$ where $G = PGO_8^+(p)$.

Q: Are there any ovoids in quadrics in $\mathbb{P}^k\mathbb{F}_q$, $k > 7$?

Q: The Leech lattice mod p does not give ovoids but ... what *does* it give?

The number of points on a quadric is divisible by the size of an ovoid. So it is natural to ask if there is a set of ovoids partitioning the points of the quadric, e.g. $(q^2+1)(q+1)$ ovoids of size q^3+1 in the triality quadric. Such a partition is called a **fan**. One can ask for fans not only in quadrics, but more generally in finite classical polar spaces.

Over the past 30 years, there has been some work on constructions and nonexistence results for fans, but only

scant literature on the subject. This should change, now that Cameron has showed us why the existence question for fans (also ovoids and spreads) is forced upon us in permutation group theory:

Theorem. *A classical group is non-synchronizing if and only if its polar space possesses either*

- *an ovoid and a spread, or*
- *a fan.*

Q: When do fans exist?

Lecture 5

p-Ranks

p-Ranks of Finite Projective Planes

Let Π be a projective plane of order n with incidence matrix A. Let p be a prime dividing n. (Only primes dividing n are of interest.) The **p-rank of Π** is the rank of A over a field of characteristic p. This is an isomorphism invariant of Π (in fact, the easiest such invariant to compute).

Since $AA^T = nI+J$, we have $\operatorname{rank}_p \Pi \leqslant \frac{1}{2}(n^2+n+2)$ whenever $p \,|\, n$. Equality holds if $p = n$.

Example: Projective Planes of order 25

There are 99 known projective planes of order 25, up to duality. Their 5-ranks are

$$226^1,\ 239^1,\ 251^1,\ 253^1,\ 255^1,\ 256^1,\ 257^1,\ 258^3,\ 259^3,$$
$$260^2,\ 261^2,\ 262^5,\ 264^2,\ 266^1,\ 268^3,\ 269^1,\ 271^1,\ 272^2,$$
$$273^1,\ 274^3,\ 275^4,\ 276^6,\ 277^6,\ 278^{12},\ 279^{27},\ 280^6,\ 286^1,\ 300^1$$

where r^k indicates k planes of rank r. The plane with smallest 5-rank is the classical plane $\mathbb{P}^2\mathbb{F}_{25}$. The largest 5-rank occurs for a derived Hughes plane.

Computation of p-rank is difficult for large matrices not because of execution time, but due to limits on available RAM.

Open Questions

Q: Does $\mathbb{P}^2\mathbb{F}_q$ have the smallest p-rank among all projective planes of order $q = p^e$? (The **Hamada-Sachar Conjecture**).

Q: Improve the upper and lower bounds for $\operatorname{rank}_p A$ in general. For $n = 25$ we know $126 \leqslant \operatorname{rank}_p A \leqslant 326$, and all known planes have p-rank in the interval $[226, 300]$.

Q: Improve the known upper bound for p-ranks of translation planes (Key and MacKenzie, 1991). For $q = 25$ this upper bound is 296; the translation planes have rank $\leqslant 264$.

The study of p-ranks of incidence matrices extends naturally to questions about Smith Normal Forms and decomposition of the associated $\mathbb{F}_p$-codes as $\mathbb{F}_pG$-modules. This work uses tools from algebraic geometry, number theory and modular representation theory. It is motivated by applications in finite geometry; but the biggest question remains the search for more such applications.

Points versus Hyperplanes

Let A be the incidence matrix of points versus hyperplanes in $\mathbb{P}^n\mathbb{F}_q$, $q{=}p^e$. Then

$$\operatorname{rank}_p A = \tbinom{p+n-1}{n}^e + 1.$$

Theorem [Blokhuis and M., 1995]**.** *If $p^{\lfloor n/2 \rfloor} > \binom{p+n-1}{n}$, then quadrics in $\mathbb{P}^n\mathbb{F}_q$ contain no ovoids.*

In particular, there are no ovoids in quadrics in $\mathbb{P}^9\mathbb{F}_{2^e}$, $\mathbb{P}^9\mathbb{F}_{3^e}$, $\mathbb{P}^{11}\mathbb{F}_{5^e}$, $\mathbb{P}^{11}\mathbb{F}_{7^e}$, etc.

Proof. If $\mathcal{O} = \{P_1, P_2, \ldots, P_m\}$ is an ovoid, then the points of $\mathcal{O}$ and the hyperplanes $P_1^\perp, \ldots, P_m^\perp$ index the rows and columns of an identity submatrix I_m in A. Comparing p-ranks,

$$m = p^{\lfloor n/2 \rfloor e} + 1 \leqslant \tbinom{p+n-1}{n}^e + 1. \qquad \square$$

We proceed to show how the latter bound can be improved.

A quadric partitions the point-hyperplane incidence matrix of $\mathbb{P}^n\mathbb{F}_q$ as

$$A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{12}^T & A_{22} \end{array}\right]$$

where rows (and columns) of A_{11} are indexed by points of the quadric (and tangent hyperplanes). Sharper bounds for ovoids follow from

$$|\mathcal{O}| = m \ \leqslant\ \operatorname{rank}_p A_{11} \ \leqslant\ \operatorname{rank}_p [A_{11}|A_{12}] \ \leqslant\ \operatorname{rank}_p A.$$

The improved bounds are sometimes tight!

Theorem [Blokhuis and M., 1995]**.**

$$\mathit{rank}_p\,[A_{11}|A_{12}] = \left[\tbinom{p+n-1}{n} - \tbinom{p+n-3}{n}\right]^e + 1.$$

So there are no ovoids in quadrics if $p^{\lfloor n/2 \rfloor} > \binom{p+n-1}{n} - \binom{p+n-3}{n}$.

We now describe three interesting instances when the improved p-rank bound is tight. Only one of these situations (ovoids in $\mathbb{P}^3\mathbb{F}_{2^e}$) has been extensively studied; and considering the strong analogy between these three situations, we conjecture that there should be lessons there which might apply to the other two cases (ovoids in quadrics in projective 6-space and 7-space).

Ovoids in Triality Quadrics of $\mathbb{P}^7\mathbb{F}_q$, $q = 2^e$

Here ovoids have size $|\mathcal{O}| = q^3 + 1 = \operatorname{rank}_2 A_{11}$. The only known examples here are:

- An infinite family of ovoids, one for each $q = 2^e$, $e \geqslant 1$. These ovoids admit $PSL_3(q)$ as an automorphism group.
- Another infinite family, one for each $q = 2^e$, e odd. These ovoids admit $PSU_3(q)$ as an automorphism group.
- One sporadic example (Dye's ovoid) for q=8.

Ovoids in Parabolic Quadrics of $\mathbb{P}^6\mathbb{F}_q$, $q = 3^e$

Here ovoids have size $|\mathcal{O}| = q^3 + 1 = \operatorname{rank}_3 A_{11}$. The only known examples here are:

- An infinite family for all $q = 3^e$, admitting $PSU_3(q)$.
- Another infinite family (the Ree-Tits ovoids) for e odd, admitting ${}^2G_2(q)$.

Ovoids of $\mathbb{P}^3\mathbb{F}_q$, $q = 2^e$

An ovoid of projective 3-space is defined somewhat differently from ovoids of quadrics or polar spaces. Here $\mathcal{O}$ is any set of $q^2 + 1$ points, no three collinear, in $\mathbb{P}^3\mathbb{F}_q$. In even characteristic, ovoids have not yet been classified, despite significant progress. However, in this case, $|\mathcal{O}| = q^2+1 = \operatorname{rank}_2 A$. The only known examples here are:

- An infinite family (elliptic quadrics), one for each $q = 2^e$, $e \geqslant 1$, admitting $PSL_2(q^2)$ as an automorphism group.
- Another infinite family (Suzuki-Tits ovoids), for e odd, admitting the Suzuki groups ${}^2B_2(q)$.

Points versus k-subspaces of $\mathbb{P}^n\mathbb{F}_q$

Let A be the incidence matrix of points versus k-subspaces of $\mathbb{P}^n\mathbb{F}_q$, $q = p^e$. Let M be the $k \times k$ matrix whose (i,j)-entry equals the coefficient of t^{pi-j} in $(1 + t + t^2 + \cdots + t^{p-1})^{n+1}$. Then

$\operatorname{rank}_p A = 1 + \big(\text{coefficient of } t^e \text{ in } tr\big[(I - tM)^{-1}\big]\big)$.

Example: Points versus Lines of $\mathbb{P}^3\mathbb{F}_{5^e}$

$(1+t+\cdots+t^4)^3$
$= 1+4t+10t^2+20t^3+35t^4+\cdots+85t^8+80t^9+\cdots+t^{16}$
so $M = \left[\begin{smallmatrix} 35 & 80 \\ 20 & 85 \end{smallmatrix}\right]$ and
$tr\big[(I - tM)^{-1}\big] = \frac{2(1-60t)}{1-120t+1375t^2}$
$=2+120t+11650t^2+1233000t^3+131941250t^4+14137575000t^5+\cdots$

so $\operatorname{rank}_5 A = 121$, 11651, etc. for $q = 5, 25, \ldots$. Hamada's Formula (1968) also expresses $\operatorname{rank}_p A$ as a complicated multiple sum, for which the execution time to evaluate is usually prohibitive.

Algebraic Sets of Points vs. Hyperplanes

Choose homogeneous coordinates $x_0, x_1, \ldots, x_n$ for $\mathbb{P}^n F$, $F = \mathbb{F}_q$, $q = p^e$. The polynomial ring $R = F[x_0, x_1, \ldots, x_n]$ is graded by degree:

$$R = \bigoplus_{k\geqslant 0} R_k = \bigoplus_{k\geqslant 0} F_k[x_0, x_1, \ldots, x_n]$$

where R_k consists of k-homogeneous polynomials. Let $\mathfrak{I} \subseteq R$ be a homogeneous ideal, i.e. $\mathfrak{I}$ is generated by a set of homogeneous polynomials. The points of $\mathbb{P}^n F$ where all $f \in \mathfrak{I}$ vanish is an **algebraic point set** $\mathcal{Z}(\mathfrak{I})$. We want to know $\operatorname{rank}_p A_{\mathfrak{I}}$ where

$$A = \left[\begin{array}{c} A_1 = A_{\mathfrak{I}} \\ \hline A_2 \end{array}\right] \Big\} \mathcal{Z}(\mathfrak{I}) \quad ;$$

here rows and columns of $A_{\mathfrak{I}}$ are indexed by points of $\mathcal{Z}(\mathfrak{I})$, and *all* hyperplanes of $\mathbb{P}^n F$.

The homogeneous ideal $\mathfrak{I} = \bigoplus_{k\geqslant 0} \mathfrak{I}_k$ is a graded R-module where $\mathfrak{I}_k = \mathfrak{I} \cap R_k$. This gives a grading of the quotient ring

$$R/\mathfrak{I} = \bigoplus_{k\geqslant 0} (R_k/\mathfrak{I}_k).$$

The **Hilbert function** of $\mathfrak{I}$ is $h_{\mathfrak{I}}(k) = \dim\big(R_k/\mathfrak{I}_k\big)$. The generating function for its sequence of values is the **Hilbert series**

$$\operatorname{Hilb}_{\mathfrak{I}}(t) = \sum_{k\geqslant 0} h_{\mathfrak{I}}(k) t^k$$

which is actually a rational function $\operatorname{Hilb}_{\mathfrak{I}}(t) \in \mathbb{Q}(t)$. That is, for $k \gg 0$, $h_{\mathfrak{I}}(k)$ coincides with a polynomial. This is the **Hilbert polynomial** of $\mathfrak{I}$, whose leading term $m\frac{k^d}{d!}$ defines the degree m and dimension d of $\mathcal{Z}(\mathfrak{I})$.

Example: Projective n-space $\mathbb{P}^n F$

The trivial ideal $\mathfrak{I} = (0)$ has zero set $\mathcal{Z}((0)) = \mathbb{P}^n F$ with Hilbert function

$$h_{(0)}(k) = \dim\big(R_k/(0)\big) = \dim R_k = \tbinom{k+n}{n}$$
$$= \tfrac{1}{n!}(k+1)(k+2)\cdots(k+n).$$

The leading term $\frac{k^n}{n!}$ tells us that $\mathbb{P}^n F$ has dimension n and degree 1. The Hilbert series is

$$\operatorname{Hilb}_{(0)}(t) = \sum_{k\geqslant 0} \binom{k+n}{n} t^k = \frac{1}{(1-t)^{n+1}}.$$

Example: Quadrics in $\mathbb{P}^n F$

A quadric $\mathcal{Z}(Q)$ is the zero set of a homogeneous quadratic polynomial $Q(x_0, x_1, \ldots, x_n) \in R_2$. Here $\mathfrak{I} = (Q)$ and $\mathfrak{I}_k = QR_{k-2}$ for $k \geqslant 2$. ($\mathfrak{I}_0 = \mathfrak{I}_1 = 0$.) The Hilbert function is

$$h_{(Q)}(k) = \begin{cases} 0, & \text{for } k = 0, 1; \\ \binom{k+n}{n} - \binom{k+n-2}{n}, & \text{for } k \geqslant 2. \end{cases}$$

The leading term $2\frac{k^{n-1}}{(n-1)!}$ tells us that the quadric has dimension $n-1$ and degree 2. The value $h_{(Q)}(p-1) = \binom{p+n-1}{n} - \binom{p+n-3}{n}$ gives $\operatorname{rank}_p A_{(Q)} = 1 + h_{(Q)}(p-1)$ over the prime field $F = \mathbb{F}_p$. The general formula for $q = p^e$ is given in the theorem above.

We have also computed $\operatorname{rank}_p A_{\mathfrak{I}}$ for several other algebraic sets $\mathcal{Z}(\mathfrak{I})$, including hermitian varieties and Grassmann varieties. In particular, we get bounds for ovoids in other finite classical polar spaces.

Disclaimer: In general, the ideal $\mathfrak{I} \subseteq R$ needs to be replaced by a slightly larger ideal:

$$\mathfrak{I} \subseteq \widehat{\mathfrak{I}} = \sqrt{\mathfrak{I} + J} \subseteq R$$

where $J = \left(x_i^q x_j - x_i x_j^q : i, j\right)$. Here $\widehat{\mathfrak{I}}$ is the set of all $f \in R$ vanishing on $\mathcal{Z}(\mathfrak{I})$. In place of $h_{\mathfrak{I}}(p-1)$ we should really have $h_{\widehat{\mathfrak{I}}}(p-1)$; but we show that in many settings, these two values agree.

Classical Generalized Quadrangles

A classical generalized quadrangle of order (q, q) has $q+1$ points on each line and $q+1$ lines through each point, $q = p^e$. Let A be its incidence matrix.

Theorem [Sastry and Sin, 1996; de Caen and M., 2000; Chandler, Sin and Xiang, 2006]**.**

- *For* $q = 2^e$, $\operatorname{rank}_p A = 1 + \left(\frac{1+\sqrt{17}}{2}\right)^{2e} + \left(\frac{1-\sqrt{17}}{2}\right)^{2e}$.
- *For* $q = p$, $\operatorname{rank}_p A = 1 + \frac{p(p+1)^2}{2}$.
- *For* $q = p^e$, p *odd*, $\operatorname{rank}_p A = 1 + \alpha_+^e + \alpha_-^e$ *where*
$$\alpha_\pm = \tfrac{p(p+1)^2}{4} \pm \tfrac{p(p^2-1)}{12}\sqrt{17}.$$

The only known generalized quadrangles of order (q, q) are the classical ones from $Sp(4, q)$ and $O(5, q)$. For $q > 4$, it is not known whether other examples exist.

Let p be prime. Any generalized quadrangle of order (n, n) has $\operatorname{rank}_p A \geqslant n^2 + 1$ (de Caen, Godsil and Royle, 1992).

The classical GQ of order $(5, 5)$ has p-rank equal to 91, for arbitrary prime p. The lower bound is 26.

Q: Improve the lower bound for p-ranks of GQ's of order (q, q).