The CRC Handbook of Combinatorial Designs

Edited by

Charles J. Colbourn

Department of Computer Science and Engineering
Arizona State University

Jeffrey H. Dinitz

Department of Mathematics and Statistics
University of Vermont

AUTHOR PREPARATION VERSION

24 October 2005

1 Finite Geometry

Leo Storme

1.1 Projective Planes

1.1 **Definition** A *finite incidence structure*, or *finite geometry*, $P = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is a finite set of *points* $\mathcal{P}$, a finite set of *lines* $\mathcal{L}$, and an *incidence* relation I between them.

1.2 **Definition** A *finite projective plane* P is a finite incidence structure such that:

1. any two distinct points are incident with exactly one line;
2. any two distinct lines are incident with exactly one point;
3. there exists a quadrangle, i.e., four points no three collinear.

1.3 **Definition** For a finite projective plane P, there is a positive integer n such that any line of P has exactly $n+1$ points. This number n is the *order* of P.

1.4 **Proposition** A finite projective plane of order n has n^2+n+1 points, n^2+n+1 lines, and $n+1$ lines through each point.

1.5 **Remark** One of the most difficult questions in finite geometry is: *what positive integers are orders of finite projective planes?* Very little is known: All known examples have prime power order. The Bruck-Ryser-Chowla theorem (§II.**??**) excludes an infinite number of integers. Only one further number has been excluded: there is no projective plane of order 10. See Remark VII.**??** for a discussion of the computer search for a projective plane of order 10.

Reference to section symmetric designs

1.6 **Table** An overview of the state of knowledge concerning small projective planes.

Reference to section computational methods

order n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
existence	y	y	y	y	n	y	y	y	n	y	?	y	n	?	y
number	1	1	1	1	0	1	1	4	0	≥ 1	?	≥ 1	0	?	≥ 22

1.7 **Theorem** Let P be a geometry consisting of a finite number of points and a finite number of at least two lines for which any two distinct points are on exactly one line, and there is an integer $n \geq 2$ such that any line has exactly $n+1$ points. Then the following assertions are equivalent:

1. P is a projective plane.
2. Any point of P is on at most $n+1$ lines.
3. Any point of P is on exactly $n+1$ lines.
4. There are exactly n^2+n+1 points in P.
5. P is a 2-$(n^2+n+1, n+1, 1)$ design (or, in other words an $S(2, n+1, n^2+n+1)$ Steiner system).

1.8 **Construction** The most important class of finite projective planes can be obtained as follows. Let V be the 3-dimensional vector space over the finite field $F = \mathbb{F}_q$ of order q. The geometry $P(V)$ that has as its *points* the 1-dimensional subspaces of V and as its *lines* the 2-dimensional subspaces of V is a projective plane.

Another way of describing this plane is as follows. Let $(a, b, c) \in V \setminus \{(0, 0, 0)\}$. Let $(a : b : c) = \{(fa, fb, fc) | f \in F \setminus \{0\}\}$. Similarly define $[x : y : z] = \{[fx, fy, fz] | f \in F \setminus \{0\}\}$ for any $(x, y, z) \in V \setminus \{(0, 0, 0)\}$. Now consider the symbols $(a : b : c)$ as points and the symbols $[x : y : z]$ as lines and say that a point $(a : b : c)$ lies on the line $[x : y : z]$ if and only if $ax + by + cz = 0$. This gives a projective plane.

These projective planes are denoted by $\mathrm{PG}(2, F)$. In addition, if $F = \mathbb{F}_q$ is a finite field of order q, then the projective plane obtained in this way has order q, and is also denoted by $\mathrm{PG}(2, q)$. Since for any prime power q there is a finite field of order q, for any prime power q there is a projective plane of order q.

1.9 Definition $(a : b : c)$ and $[x : y : z]$ are the *homogeneous coordinates* of the corresponding point and line of $\mathrm{PG}(2, F)$.

1.10 Remark The finite projective planes $\mathrm{PG}(2, F)$ are exactly the finite *desarguesian* projective planes, i.e. those finite projective planes in which the theorem of Desargues is valid (Theorem 1.152). Equivalently, the finite projective planes $\mathrm{PG}(2, F)$ are precisely those finite projective planes that can be embedded as a plane in a higher-dimensional projective space.

Sections 1.14 to 1.22 discuss nondesarguesian projective planes.

1.2 Affine Planes

1.11 Definition A *finite affine plane* is a finite incidence structure such that:

1. any two distinct points are on exactly one line;
2. for any point P outside a line ℓ there is exactly one line through P that has no point in common with ℓ. (This is the *euclidean parallel axiom*);
3. there exist three points not on a common line.

1.12 Remark If one defines a *parallelism* among the lines by saying that two lines are parallel if they are equal or have no point in common, then the parallelism of an affine plane is an equivalence relation such that any two nonparallel lines meet. The equivalence classes belonging to the parallelism are *parallel classes*. By axiom (2), any parallel class of an affine plane is a partition of the point set by lines.

1.13 Construction Given an affine plane A one can define as follows a new geometry P: the points of P are the points of A and the parallel classes of A; the lines of P are the lines of A and one new line $g^\star$. The incidence is defined as follows: line $g^\star$ is incident with all parallel classes, and each line ℓ of A is now incident with its points in A together with the parallel class to which it belongs. Then P is a projective plane. Conversely, if one removes a line g together with all its points from a projective plane P one gets an affine plane $A = P_g$. Two lines of the affine plane P_g are parallel if and only if the projective lines containing them meet the line g in the same point. We call g the *infinite line* of A and the points of g the *infinite points* of A.

1.14 Definition For a finite affine plane A, there is a positive integer n such that any line of A has exactly n points. This number n, which is also the order of the corresponding projective plane, is the *order* of A.

1.15 Proposition A finite affine plane of order n has n^2 points, $n^2 + n$ lines, and $n + 1$ lines through each point.

1.16 Theorem Let A be a finite geometry consisting of points and at least two lines for which any two distinct points are on exactly one line, and there is an integer $n \geq 2$ such that any line has exactly n points. Then the following assertions are equivalent:

1. A is an affine plane.
2. Any point of A is on exactly $n+1$ lines.
3. There are exactly n^2 points in A.
4. A is a 2-$(n^2, n, 1)$ design (equivalently, an $S(2, n, n^2)$ Steiner system).

1.17 Construction The usual way to construct finite affine planes is as follows. Let F be a finite field $\mathbb{F}_q$. Then the geometry $\mathrm{AG}(2, F)$ has as points the pairs (a, b) with $a, b \in F$, and its lines are the sets of points (x, y) satisfying an equation $Y = mX + b$ $(m, b \in F)$ or an equation $X = c$ with $c \in F$. Then $\mathrm{AG}(2, F)$ is an affine plane.

Another way of describing this affine plane is as follows. Let V be a 2-dimensional vector space over F. The points of $\mathrm{AG}(2, F)$ are all vectors of V and the lines are all cosets $v + \langle u \rangle$, where $u \in V \backslash \{(0, 0)\}$. If F is a finite field with q elements, then $\mathrm{AG}(2, F)$ is an affine plane of order q, and is also denoted by $\mathrm{AG}(2, q)$.

1.18 Remark The finite affine planes $\mathrm{AG}(2, F)$ are precisely the finite *desarguesian* affine planes and the finite affine planes $\mathrm{AG}(2, F)$ are precisely those finite affine planes that can be embedded in a higher-dimensional affine space. See §1.4.

1.19 Remark The finite affine planes are classical examples of quasi-residual designs which effectively are residual designs (§I.**??**), and are classical examples of resolvable designs (§I.**??**).

Reference to residual designs in section on symmetric designs

Reference to resolvable designs section

1.3 Projective Spaces

1.20 Definition A *finite projective space* P is a finite incidence structure such that:

1. any two distinct points are on exactly one line;
2. (*Veblen-Young axiom*) let A, B, C, D be four distinct points of which no three are collinear. If the lines AB and CD intersect each other, then the lines AD and BC also intersect each other;
3. any line has at least three points.

1.21 Examples Finite projective spaces can be obtained as follows. Let V be a vector space of dimension $d+1$ over the finite field $F = \mathbb{F}_q$. The geometry $P(V)$ that has as its *points* the 1-dimensional subspaces of V and as its *lines* the 2-dimensional subspaces of V is a finite projective space.

Another way of describing the same geometry is as follows. Let $d+1$ be a positive integer and F a finite field $\mathbb{F}_q$. Let $(a_0, a_1, \ldots, a_d) \in V \setminus \{(0, 0, \ldots, 0)\}$. Let $(a_0 : a_1 : \ldots : a_d) = \{(fa_0, fa_1, \ldots, fa_d) | f \in F \setminus \{0\}\}$. The symbols $(a_0 : a_1 : \ldots : a_d)$ are considered as points and are called *homogeneous coordinates*. The line through $(a_0 : a_1 : \ldots : a_d)$ and $(b_0 : b_1 : \ldots : b_d)$ is the set of points

$$\{(b_0 : b_1 : \ldots : b_d)\} \cup \{(a_0 + cb_0 : a_1 + cb_1 : \ldots : a_d + cb_d) \mid c \in F\}.$$

The projective space $P(V)$ is also denoted by $\mathrm{PG}(d, F)$. If F is a finite field with q elements, then we also write $\mathrm{PG}(d, q)$ instead of $\mathrm{PG}(d, F)$.

1.22 Theorem (*Representation theorem of projective geometry*) Any finite projective space that is not a projective plane is isomorphic to some $P(V)$.

1.23 Definition Let P be a projective space. A *(linear) subspace* of P is a set U of points of P such that for any two points $P, Q \in U$, any point on the line PQ also is contained in U. Any subspace is, together with the lines contained in it, a projective space.

1.24 Definition If S is an arbitrary set of points of P, then the *span* $\langle S \rangle$ of S is the intersection of all subspaces containing S. The span $\langle S \rangle$ is again a subspace.

1.25 Definition A set S of points of P is *independent* if for any $x \in S$, $x \notin \langle S \setminus \{x\} \rangle$. An independent set that spans a projective space P is a *basis* of P.

1.26 Theorem Let U be a subspace of P, and let $Q \in P \setminus U$. Then the subspace W spanned by U and Q consists precisely of the points on the lines QX with $X \in U$.

1.27 Remark A set of points is a basis if and only if it is a maximal independent set if and only if it is a minimal spanning set. All bases have the same number of elements.

1.28 Definition A projective space P has *dimension* d if a basis has $d+1$ elements. A subspace of dimension 2 is a *plane*; in a d-dimensional projective space, the *hyperplanes* are the subspaces of dimension $d-1$.

1.29 Proposition (*Dimension formula*) For two subspaces U_1 and U_2: $\dim(\langle U_1, U_2 \rangle) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2)$. In particular, any t-dimensional subspace not contained in a hyperplane H intersects H in a subspace of dimension $t-1$.

1.30 Definition The *quotient geometry* (or *residual geometry*) P/U of a projective space P modulo a t-dimensional subspace U has as points the $(t+1)$-dimensional subspaces through U, and as lines the $(t+2)$-dimensional subspaces through U.

1.31 Proposition If P has dimension d and U is a t-dimensional subspace, then P/U is a projective space of dimension $d-t-1$.

1.32 Definition If P is finite, there is an integer $n \geq 2$ such that any line has exactly $n+1$ points. This number n is the *order* of P.

1.33 Remark Let P be a finite d-dimensional projective space of order n. There are $n^t + \cdots + n + 1$ points in a t-dimensional subspace of P. The number of points and the number of hyperplanes of P are both equal to $n^d + \cdots + n + 1$. Any subspace and any quotient geometry of P also have order n.

1.34 Proposition Let q be a prime power, and d and i positive integers with $i \leq d$. The *gaussian coefficients*

$$\begin{bmatrix} d \\ i \end{bmatrix}_q = \frac{(q^d-1)(q^{d-1}-1)\cdots(q^{d-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}$$

denote the number of i-dimensional vector subspaces of a d-dimensional vector space over $\mathbb{F}_q$.

1.35 Definition The points of $\mathrm{PG}(d,q)$ together with the i-dimensional subspaces of $\mathrm{PG}(d,q)$ as blocks and incidence by natural containment form an incidence structure denoted by $\mathrm{PG}_i(d,q)$.

1.36 Proposition $\mathrm{PG}_i(d,q)$ is a block design with parameters

$$v = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = (q^{d+1}-1)/(q-1),\ k = \begin{bmatrix} i+1 \\ 1 \end{bmatrix}_q = (q^{i+1}-1)/(q-1),\ \lambda = \begin{bmatrix} d-1 \\ i-1 \end{bmatrix}_q$$

(also $b = \begin{bmatrix} d+1 \\ i+1 \end{bmatrix}_q$ and $r = \begin{bmatrix} d \\ i \end{bmatrix}_q$).

1.4 Affine Spaces

1.37 Definition A *parallelism* of a geometry consisting of a set of points and a set B of blocks is an equivalence relation ("parallel") on B that satisfies the *euclidean parallel axiom*: for any point P and any block B there is exactly one block C through P that is parallel to B. The equivalence classes of a parallelism are *parallel classes*.

1.38 Definition A *finite affine space* is a finite incidence structure A such that:

1. any two distinct points are on exactly one line;
2. A has a parallelism;
3. (*Triangle axiom*) if A, B, C are three noncollinear points and A', B' are two distinct points such that the line $A'B'$ is parallel to AB, then the line on A' parallel to AC and the line on B' parallel to BC intersect in some point C';
4. there exist three points not on a common line.

1.39 Remark Most properties of affine spaces follow from the fact that they have a *projective closure*: for any affine space A there exists a projective space P and a hyperplane H of P such that A consists precisely of the points and lines not contained in H. Also, two lines of A are parallel if and only if they meet in the same point of H. The hyperplane H is the *hyperplane at infinity* of A.

1.40 Definition For a finite affine space A, there is a positive integer n such that any line of A has exactly n points. This number n is the *order* of A. The *dimension* of an affine space is the dimension of the corresponding projective space.

1.41 Theorem Let A be a finite affine space of dimension d and order n.

1. The number of points of A is n^d.
2. If U is a t-dimensional subspace of A, then the quotient geometry A/U is a projective space of dimension $d-t-1$ and order n.

1.42 Definition $\mathrm{AG}(d,q)$ denotes the affine space of dimension d and order q with projective closure equal to $\mathrm{PG}(d,q)$.

1.43 Definition In $\mathrm{AG}(d,q)$ the cosets of $\{\bar{0}\}$ are *points*, those of 1-dimensional spaces *lines*, those of $(d-1)$-dimensional spaces *hyperplanes*; in general, the cosets of i-dimensional subspaces are *i-flats*. The points of $\mathrm{AG}(d,q)$ together with the i-dimensional flats of $\mathrm{AG}(d,q)$ as blocks and incidence by natural containment form an incidence structure denoted by $\mathrm{AG}_i(d,q)$.

1.44 Proposition $\mathrm{AG}_i(d,q)$ is a block design with parameters $v=q^d$, $k=q^i$ and $\lambda = \begin{bmatrix} d-1 \\ i-1 \end{bmatrix}_q$ (also $b = q^{d-i}\begin{bmatrix} d \\ i \end{bmatrix}_q$ and $r = \begin{bmatrix} d \\ i \end{bmatrix}_q$).

1.45 Theorem (Buekenhout) Let A be a linear space that contains at least one line with at least four points. If any three noncollinear points generate an affine plane, then A is an affine space.

1.46 Remark Theorem 1.45 is false if one drops the hypothesis that there is a line with at least four points. Hall triple systems (§IV.**??**) give examples in which all lines have size three.

reference to Hall triple systems

1.5 Subplanes

1.47 **Definition** Let P be a projective plane with point set $\mathcal{P}$ and line set $\mathcal{L}$. A projective plane P' with point set $\mathcal{P}'$ and line set $\mathcal{L}'$ is a *subplane* of P if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$, and P' inherits the incidence relation from P.

1.48 **Theorem** (Bruck) Let P be a finite projective plane of order n, and let P' be a subplane of order $m < n$ of P. Then $n = m^2$ or $m^2 + m \leq n$.

1.49 **Definition** A subplane of order m of a projective plane of order $n = m^2$ is a *Baer subplane.*

1.50 **Theorem** Let P be a finite projective plane of order n, and let P' be a subplane of order $m < n$ of P. Then the following assertions are equivalent:

1. P' is a Baer subplane of P;
2. any point outside P' is on exactly one line of P';
3. any line not in P' has exactly one point in common with P'.

1.51 **Remarks** Let $P = \mathrm{PG}(2, F)$, with F the field $\mathbb{F}_q$. Let K be a subfield of F and consider the geometry P' consisting of the homogeneous coordinates for points and lines whose entries are in K. Then P' is a subplane of P.

The subfields of a finite field $\mathbb{F}_{p^a}$, where p is a prime, are precisely those fields $\mathbb{F}_{p^b}$ where b divides a. The subplanes of a projective plane $\mathrm{PG}(2, p^a)$, with p a prime, are exactly the projective planes $\mathrm{PG}(2, p^b)$ where b divides a.

1.52 **Proposition** A projective plane $\mathrm{PG}(2, q)$ has a Baer subplane if and only if q is a square.

1.6 Baer Subgeometries

1.53 **Definition** Let P be a projective space with point set $\mathcal{P}$ and line set $\mathcal{L}$. A projective space P' with point set $\mathcal{P}'$ and line set $\mathcal{L}'$ is a *subgeometry* of P if $\mathcal{P}' \subseteq \mathcal{P}$ and $\mathcal{L}' \subseteq \mathcal{L}$, and $\mathcal{P}'$ inherits the incidence relation of $\mathcal{P}$.

1.54 **Proposition** (Bruck) Let P be a finite projective space of dimension d and order q. Let P' be a subgeometry of P of order q'. If $q' < q$, then $q' \leq \sqrt{q}$.

1.55 **Definition** A d-dimensional subgeometry of $\mathrm{PG}(d, q)$, whose order is $\sqrt{q}$, is a *Baer subgeometry* of $\mathrm{PG}(d, q)$.

1.56 **Theorem** If $P = P(V)$ is a finite desarguesian projective space of order $q = p^n$, p prime, then P has a subgeometry of order q' if and only if $q' = p^m$ with $m \mid n$. In particular, P has a Baer subgeometry if and only if q is a square.

New theorem **1.57** **Theorem** Let B be a Baer subgeometry of $P = \mathrm{PG}(d, q)$.

1. If U is an i-dimensional subspace of P that intersects B in a j-dimensional subspace, then there is precisely one subspace of dimension $2i - j$ of B containing U. In particular, if U has no point in common with B, then U is contained in a unique $(2i + 1)$-dimensional subspace of B. So, any point of $P \setminus B$ lies on a unique line of B.
2. Any subspace of dimension $d - i$ of P contains at least one subspace of dimension $d - 2i$ of B; this bound is sharp.

1.7 Collineations

1.58 Definition Let P be a projective space of dimension at least two. A *collineation* (*automorphism*) of P is a bijective map α on the point set of P that preserves collinearity; that is, P, Q, R collinear implies $\alpha(P)$, $\alpha(Q)$, $\alpha(R)$ collinear. All collineations of P form the *full collineation group* $\mathrm{Aut}P$ of P. A *collineation group* of P is a subgroup of $\mathrm{Aut}P$.

1.59 Definition Let $P = P(V)$ be a projective space defined over the F-vector space V. A *semilinear map* of V is a map $f : V \to V$ together with an automorphism σ of F such that $f(v + w) = f(v) + f(w)$ for all $v, w \in V$, and $f(a \cdot v) = \sigma(a) \cdot f(v)$ for all $a \in F$, $v \in V$.

1.60 Theorem (*Fundamental theorem of projective geometry*) Any invertible semilinear map of V induces a collineation of $P(V)$. Conversely, any collineation of $P(V)$, $\dim V \geq 3$, is induced by an invertible semilinear map.

1.61 Definition The group of all collineations of the d-dimensional projective space $P(V) = \mathrm{PG}(d, F)$, $d \geq 2$, is denoted by $\mathrm{P\Gamma L}(d + 1, F)$. The set $\mathrm{PGL}(d + 1, F)$ of collineations that are induced by invertible linear maps of V is a normal subgroup of $\mathrm{P\Gamma L}(d+1, F)$. The set of collineations $\mathrm{PSL}(d + 1, F)$ induced by linear maps with determinant 1 is a group of collineations, the *little projective group* of $P(V)$.

1.62 Definition Let P be a projective space. A collineation α of P is a *central collineation* if there exists a point C (the *center*) and a hyperplane H (the *axis*) such that α fixes any line on C and any point on H. If α is a central collineation different from the identity, its center and axis are uniquely determined. A central collineation different from the identity, with center C and axis H, is an *elation* if $C \in H$ and a *homology* otherwise.

1.63 Definition A *Baer collineation* is a collineation that fixes a Baer subgeometry pointwise.

1.64 Theorem (Baer) A collineation of order 2 of a projective space is either a central collineation or a Baer collineation.

1.65 Theorem The number of fixed points of a collineation of P equals the number of fixed hyperplanes of P.

1.66 Theorem Let G be an arbitrary automorphism group of a finite projective space P.

1. The number of point orbits of P equals the number of hyperplane orbits.
2. The group G is point-transitive if and only if it is transitive on the hyperplanes.
3. The group G is 2-fold transitive on the points of P if and only if it is 2-fold transitive on the hyperplanes of P.

1.8 Spreads

1.67 Definition Let t and d be positive integers with $t < d$. A *t-spread* in a d-dimensional projective space P is a set S of t-dimensional subspaces such that any point of P is on exactly one element of S.

1.68 Theorem A finite projective space $P = \mathrm{PG}(d, q)$ contains a t-spread if and only if $(t+1)|(d+1)$. In particular, $\mathrm{PG}(d, q)$ contains a spread of lines if and only if d is odd.

1.69 Construction One construction for t-spreads is as follows. Let t and d be positive integers such that $(t+1)|(d+1)$. Let q be a prime power. Then the field $F^\star = \mathbb{F}_{q^{d+1}}$ of order q^{d+1} contains $F = \mathbb{F}_{q^{t+1}}$ as a subfield. Consider $F^\star$ as an F-vector space. Then the set of 1-dimensional subspaces of $F^\star$ over F forms a t-spread in the d-dimensional projective space associated to the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^{d+1}}$. The t-spreads obtained in this way are *regular* (See Definition 1.73).

definition number was wrong is now corrected

1.70 Definition A *t-regulus* of $\mathrm{PG}(2t+1,q)$ is a set R of $q+1$ mutually skew t-dimensional subspaces such that any line intersecting three elements of R intersects all elements of R. These lines are *transversals* of R.

1.71 Proposition Any three mutually skew t-dimensional subspaces of $\mathrm{PG}(2t+1,q)$ determine a unique t-regulus containing them.

1.72 Remark The points covered by a 1-regulus in $\mathrm{PG}(3,q)$ are the points of a hyperbolic quadric.

1.73 Definition A t-spread S in $\mathrm{PG}(2t+1,q)$ is *regular* if for any three elements of S, the t-regulus determined by them is also contained in S. In general, a t-spread S of $P = \mathrm{PG}(d,q)$ is *regular*, if for any two elements U, W of S, S induces a regular t-spread in $\langle U,W\rangle$.

1.74 Theorem A finite projective space $P = \mathrm{PG}(d,q)$ contains a regular t-spread if and only if $t+1$ divides $d+1$.

1.75 Remark There are many spreads that are not regular. One class of examples is obtained as follows. Let $t=1$. First of all, the set of transversals of a 1-regulus R is again a 1-regulus, the *opposite* 1-regulus of R. Start with a regular 1-spread S_0. Replace one 1-regulus of S_0 by its opposite 1-regulus to obtain a 1-spread S_1. If S_1 contains a 1-regulus, replace this 1-regulus by its opposite 1-regulus to obtain S_2. Continue in this manner. Any 1-spread so obtained is called *subregular.*

1.9 Arcs, Ovals, Hyperovals and Normal Rational Curves

1.76 Definition A *k-arc* in a projective plane is a set of k points, no three collinear.

1.77 Theorem If a projective plane of order q has a k-arc, then $k \le q+2$. If $k = q+2$, then q is even.

1.78 Definition Let P be a projective plane of order q. An *oval* of P is a $(q+1)$-arc, and a *hyperoval* is a $(q+2)$-arc.

1.79 Examples The *conics* are examples of ovals in $\mathrm{PG}(2,q)$. Let $\mathrm{PG}(2,q)$ be described by homogeneous coordinates. Then a conic is the set of points $(x:y:z)$ satisfying a quadratic equation equivalent to $x^2 = yz$.

1.80 Theorem (Segre) In $\mathrm{PG}(2,q)$, q odd, every oval is a conic.

1.81 Proposition Any oval in a projective plane of even order q can uniquely be extended to a hyperoval. The reason for this is that for q even all tangents to a $(q+1)$-arc pass through a common point, the *nucleus* of the $(q+1)$-arc.

1.82 Examples The *regular* hyperovals which consist of the union of a conic and its nucleus are the classical examples of hyperovals in $\mathrm{PG}(2,q)$, q even. In $\mathrm{PG}(2,q)$, q even, $q \ge 16$, infinite classes of *non-regular hyperovals* are known. Every hyperoval in $\mathrm{PG}(2,q)$, q

even, is projectively equivalent to a hyperoval $\{(1 : x : F(x)) | x \in \mathbb{F}_q\} \cup \{(0 : 1 : 0), (0 : 0 : 1)\}$, for some polynomial F with $F(0) = 0$ and $F(1) = 1$. Next to the infinite classes of hyperovals presented in the next table, there also exists a sporadic hyperoval in PG$(2, 32)$.

1.83 Table [17] Infinite classes of hyperovals.

Name	$F(X)$	$q = 2^h$	Conditions
Regular	X^2		
Translation	X^{2^i}		$(h, i) = 1$
Segre	X^6	h odd	
Glynn I	$X^{3\sigma+4}$	h odd	$\sigma = 2^{(h+1)/2}$
Glynn II	$X^{\sigma+\lambda}$	h odd	$\sigma = 2^{(h+1)/2}; \lambda = 2^m$ if $h = 4m - 1$; $\lambda = 2^{3m+1}$ if $h = 4m + 1$
Payne	$P(X)$	h odd	
Cherowitzo	$C(X)$	h odd	$\sigma = 2^{(h+1)/2}$
Subiaco	$S_1(X)$	$h = 4r + 2$	$\omega^2 + \omega + 1 = 0$
Subiaco	$S_2(X)$	$h = 4r + 2$	$\delta = \zeta^{q-1} + \zeta^{1-q}; \zeta$ primitive in $\mathbb{F}_{q^2}$
Subiaco	$S_3(X)$	$h \neq 4r + 2$	$T_2(1/\delta) = 1$
Adelaide	$S(X)$	h even, $h \geq 4$	$\beta \in \mathbb{F}_{q^2} \setminus \{1\},\ \beta^{q+1} = 1, T(x) = x + x^q$, $m \equiv \pm(q-1)/3 \pmod{q+1}$

Where $P(X) = X^{1/6} + X^{3/6} + X^{5/6}$; $C(X) = X^\sigma + X^{\sigma+2} + X^{3\sigma+4}$;

$S_1(X) = \frac{\omega^2(X^4+X)}{X^4+\omega^2X^2+1} + X^{1/2}$; $S_2(X) = \frac{\delta^2X^4+\delta^5X^3+\delta^2X^2+\delta^3X}{X^4+\delta^2X^2+1} + \left(\frac{X}{\delta}\right)^{1/2}$;

$S_3(X) = \frac{(\delta^4+\delta^2)X^3+\delta^3X^3+\delta^2X}{X^4+\delta^2X^2+1} + \left(\frac{X}{\delta}\right)^{1/2}$; and

$S(X) = \frac{T(\beta^m)(X+1)}{T(\beta)} + \frac{T((\beta X+\beta^q)^m)}{T(\beta)(X+T(\beta)X^{1/2}+1)^{m-1}} + X^{1/2}$.

The function T_2 stands for the *trace function* $T_2 : \mathbb{F}_{2^h} \to \mathbb{F}_2 : x \mapsto \sum_{i=0}^{h-1} x^{2^i}$.

1.84 Theorem In PG$(2, 2)$, PG$(2, 4)$ and PG$(2, 8)$, every hyperoval is regular. In PG$(2, 16)$, there exist exactly two distinct hyperovals: the regular hyperoval and the Subiaco hyperoval, also called the *Lunelli-Sce hyperoval*. In PG$(2, 32)$, there exist exactly six distinct hyperovals: the regular hyperoval, the translation hyperoval defined by $F(X) = X^4$, the Segre hyperoval, the Payne hyperoval, the Cherowitzo hyperoval, and the sporadic *O'Keefe-Penttila hyperoval*.

1.85 Definition A k-arc of PG$(2, q)$ is *complete* if it is not properly contained in a $(k+1)$-arc of PG$(2, q)$.

1.86 Table [17] Extendability of arcs to larger arcs. Any k-arc, with $k > k_0$, in PG$(2, q)$ is contained in a K_0-arc of PG$(2, q)$. In the table, for $q = 2^{2e}$, $e > 2$, two possible values for K_0 occur since in any projective plane PG$(2, q)$, $q > 4$ square, there exists a complete $(q - \sqrt{q} + 1)$-arc. Here, p always is a prime.

q	k_0	K_0
$q = p^{2e},\ p > 2,\ e \geq 1$	$q - \sqrt{q}/4 + 25/16$	$q + 1$
$q = p^{2e+1},\ p > 2,\ e \geq 1$	$q - \sqrt{pq}/4 + 29p/16 + 1$	$q + 1$
q prime, $q > 2$	$44q/45 + 8/9$	$q + 1$
$q = p^h,\ p \geq 5$	$q - \sqrt{q}/2 + 5$	$q + 1$
$q = p^h,\ p \geq 3,\ q \geq 23^2$, $q \neq 5^5,\ 3^6,\ h$ even for $p = 3$	$q - \sqrt{q}/2 + 3$	$q + 1$
$q = 2^{2e},\ e > 2$	$q - 2\sqrt{q} + 6$	$q + 2$ or $q - \sqrt{q} + 1$
$q = 2^{2e+1},\ e \geq 1$	$q - \sqrt{2q} + 2$	$q + 2$

New table **1.87** **Table** [17] Exact values for $m'(2,q)$, the size of the second largest complete arcs in $PG(2,q)$, for small values of q.

q	7	8	9	11	13	16	17	19	23	25	27	29
$m'(2,q)$	6	6	8	10	12	13	14	14	17	21	22	24

New theorem **1.88** **Theorem** In $PG(2,q)$, $q=2^h$, h even, $h \geq 4$, $m'(2,q) = q - \sqrt{q} + 1$.

Definition extended **1.89** **Definition** A k-*arc* in $PG(d,q)$ is a set of k points, no $d+1$ dependent. A k-arc of $PG(d,q)$ is *complete* if it is not properly contained in a $(k+1)$-arc of $PG(d,q)$.

1.90 **Table** [17] The value of $m(d,q)$, the size of the largest arcs in $PG(d,q)$, for small dimensions d. The characterization of the $m(d,q)$-arcs L in $PG(d,q)$ is given in the last column.

q	d	$m(d,q)$	L
$q=p^h$	$d \geq q-1$	$d+2$	$\{e_0,\ldots,e_d,e\}$
q odd, $q>3$	3	$q+1$	NRC
$q=2^h$, $q>4$	3	$q+1$	L_e, $e=2^v$, $(v,h)=1$
q odd, $q>5$	4	$q+1$	NRC for $q>83$
$q=2^h$, $q>4$	4	$q+1$	NRC
$q=2^h$, $q\geq 8$	5	$q+1$	NRC for $q \geq 16$
$q=2^h$, $q\geq 16$	6	$q+1$	NRC for $q>64$

Where, $e_0 = (1:0:\ldots:0), e_1 = (0:1:0:\ldots:0),\ldots,e_d = (0:0:\ldots:0:1)$ and $e=(1:\ldots:1)$. *NRC* stands for *normal rational curve*, that is, a $(q+1)$-arc in $PG(d,q)$, $2 \leq d \leq q-2$, equivalent to the $(q+1)$-arc $\{(1:t:\ldots:t^d) | t \in \mathbb{F}_q^+\}$, where $\mathbb{F}_q^+ = \mathbb{F}_q \cup \{\infty\}$ and where $t=\infty$ defines the point e_d. In $PG(3,q)$, $q=2^h$, $h>2$, $L_e = \{(1:t:t^e:t^{e+1})|t \in \mathbb{F}_q^+\}$, with $e=2^v$, $(v,h)=1$, and with $t=\infty$ defining the point $e_3=(0:0:0:1)$.

1.91 **Table** [17] Extendability of arcs to larger arcs in $PG(d,q)$. Any k-arc in $PG(d,q)$, with k larger than the value in column three is extendable to a $(q+1)$-arc L in $PG(d,q)$ which is either a normal rational curve or a $(q+1)$-arc equivalent to L_e (Table 1.90). The type of the $(q+1)$-arc L is denoted in the fourth column. Here, p is a prime.

d	q	$q+1 \geq k >$	L
≥ 2	$q=p^{2e}$, p odd, $e\geq 1$	$q-\sqrt{q}/4+d-7/16$	NRC
≥ 2	$q=p^{2e+1}$, p odd, $e \geq 1$	$q-\sqrt{pq}/4+29p/16+d-1$	NRC
≥ 2	q prime, $q>2$	$44q/45+d-10/9$	NRC
≥ 2	$q=p^h$, $p\geq 5$	$q-\sqrt{q}/2+d+3$	NRC
≥ 2	$q=p^h$, $p\geq 3$, $q \geq 23^2$, h even for $p=3$, $q \neq 5^5$, 3^6	$q-\sqrt{q}/2+d+1$	NRC
3	$q=2^h, h>1$	$q-\sqrt{q}/2+9/4$	L_e
≥ 4	$q=2^h$, $h>2$	$q-\sqrt{q}/2+d-3/4$	NRC

New table **1.92** **Table** [17] Values of k for which there exist complete k-arcs in the respective spaces $PG(d,q)$, d large. The last column indicates when the $(q+1)$-arcs in these spaces are always normal rational curves (NRC). Here, p is a prime.

q	d	$k \in$	$(q+1)$-arc
$q = p^{2e},\ e \geq 1,\ p > 2$	$q-2 \geq d > q - \sqrt{q}/4 - 39/16$	$\{q+1\}$	NRC
$q = p^{2e+1},\ e \geq 1,\ p > 2$	$q-2 \geq d > q - \sqrt{pq}/4 + 29p/16 - 3$	$\{q+1\}$	NRC
q prime, $q > 2$	$q-2 \geq d > 44q/45 - 28/9$	$\{q+1\}$	NRC
$q = p^h,\ p \geq 5$	$q-2 \geq d > q - \sqrt{q}/2 + 1$	$\{q+1\}$	NRC
$q = p^h,\ p \geq 3,\ q \neq 5^5,\ 3^6,$ $q \geq 23^2,\ h$ even for $p = 3$	$q-2 \geq d > q - \sqrt{q}/2 - 1$	$\{q+1\}$	NRC
$q = 2^h,\ q \geq 32,\ q \neq 64$	$q-5 \geq d > q - \sqrt{q}/2 - 11/4$	$\{d+4,$ $d+5,\ q+1\}$	NRC
$q = 64$	$d = 58$ or $d = 59$	$\{d+4,\ q+1\}$	NRC
$q = 2^h,\ q \geq 8$	$q-4$	$\{q,\ q+1\}$	
$q = 2^h,\ q \geq 8$	$q-3$	$\{q+1\}$	
$q = 2^h,\ q \geq 4$	$q-2$	$\{q+2\}$	

1.93 **Table** [17] Value of $m'(3,q)$, the size of the second largest complete k-arcs in PG$(3,q)$, for small q. New table

q	8	9	11	13	16	17	19	25
$m'(3,q)$	7	9	9	10	12	13	14	18

1.94 **Table** [17] For the indicated spaces PG(d,q), $2 \leq d \leq q-2$, it is stated if every $(q+1)$-arc is a normal rational curve (NRC), the values of d for which $m(d,q) = q+1$, and if there exist $(q+2)$-arcs. New table

q	$(q+1)$-arc = NRC	$m(d,q) = q+1$	$(q+2)$-arcs
$5 \leq q \leq 27,\ q \neq 9,\ q$ odd	$d \in \{2,\ldots,q-2\}$	$d \in \{2,\ldots,q-2\}$	
$8, 16$	$d \in \{3,\ldots,q-4\}$	$d \in \{3,\ldots,q-3\}$	$d \in \{2, q-2\}$
9	$d \in \{2,3\} \cup \{5,6,7\}$	$d \in \{2,\ldots,7\}$	

1.95 **Remark** The following theorem presents the only $(q+1)$-arc in PG(d,q), $2 \leq d \leq q-2$, q odd, different from a normal rational curve, presently known.

1.96 **Theorem** (Glynn) In PG$(4,9)$, a 10-arc is either a normal rational curve or a 10-arc projectively equivalent to the 10-arc $L = \{(1 : t : t^2 + \eta t^6 : t^3 : t^4) | t \in \mathbb{F}_9\} \cup \{(0 : 0 : 0 : 0 : 1)\}$, where $\eta^4 = -1$.

1.10 $\{k;r\}$-Arcs

1.97 **Definition** A $\{k;r\}$-*arc* in a projective plane is a set K of k points such that r is the maximum number of points in K that are collinear. A $\{k;2\}$-arc is a k-*arc*.

1.98 **Theorem** (Barlotti) Let K be a $\{k;r\}$-arc in a projective plane of order q. Then $k \leq (q+1)(r-1)+1$.

1.99 **Definition** The $\{k;r\}$-arcs for which $k = (q+1)(r-1)+1$ are *maximal* $\{k;\ r\}$*-arcs*.

1.100 **Examples** The singletons ($k = r = 1$) and the whole plane ($r = q+1$) are *trivial* maximal $\{k;r\}$-arcs. The hyperovals are nontrivial maximal $\{k;r\}$-arcs.

1.101 **Lemma** (Barlotti) If a projective plane of order q contains a maximal $\{k;r\}$-arc, then r must be a divisor of q.

1.102 Theorem (Ball, Blokhuis and Mazzocca) If $\mathrm{PG}(2,q)$ contains a nontrivial maximal $\{k;r\}$-arc, then q is even.

1.103 Theorem (Denniston) In $\mathrm{PG}(2,q)$, $q=2^h$, for any $r=2^{h'}$ with $0 \le h' \le h$, there exists a maximal $\{k;r\}$-arc.

1.104 Remark The construction method of Denniston for maximal $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$, q even, was generalized by Mathon [23]. Hamilton and Mathon used this generalized method to construct many new maximal $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$, q even [13].

fix spacing

1.105 Table [17] Known exact values for $m_r(2,q)$, the size of the largest $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$.

r	$q=p^h,\ p$ prime	$m_r(2,q)$
2	q odd	$q+1$
2^e	2^h	$(2^e-1)q+2^e$
$\sqrt{q}+1$	q square, $q \ge 25$	$q\sqrt{q}+1$
$(q+1)/2$	q odd prime	$(q^2-q)/2+1$
$(q+3)/2$	q odd prime	$(q^2+q)/2+1$
q	q	q^2
$q-1$	q square, $q>4$	$q^2-q-2\sqrt{q}-1$
$q-2$	q odd square, $q>121$	$q^2-2q-3\sqrt{q}-2$
$q+1-t$, $t>1$	$q=p^{2e}$, $p>3$, $t<\min(q^{1/6},q^{1/4}/2)$	$q^2+q+1-t(q+\sqrt{q}+1)$
$q+1-t$, $t>1$	$q=p^{2e}$, $p=2,3$, $t<\min(2^{-1/3}q^{1/6},q^{1/4}/2)$	$q^2+q+1-t(q+\sqrt{q}+1)$

1.106 Table [17] Lower bounds on $m_r(2,q)$.

r	q	$m_r(2,q) \ge$
$r=3$	q exceptional	$q+\lfloor 2\sqrt{q} \rfloor$
$r=\sqrt{q}+1$	q square	$(r-1)q+1$
$r=(q+1)/2$	q odd	$(r-1)q+1$
$r=(q+3)/2$	q odd	$(r-1)q+1$
$r=q-1$	q	$(r-1)q+1$
$r=q-2$	q even	$(r-1)q+2$
r	q square	$(r-1)q+r-\sqrt{q}+\sqrt{q}(r-q)$
$r=q-\sqrt{q}$	q square	$(r-1)q+\sqrt{q}$
$(q-r)\mid q$	q	$(r-1)q+q-r$

1.107 Remark A major problem is the construction of *large* $\{k;r\}$-arcs in $\mathrm{PG}(2,q)$. Since the union of t conics is a $\{k;2t\}$-arc, it follows that $m_r(2,q) \ge \lfloor r/2 \rfloor (q+1)$. Hirschfeld and Szőnyi [18] proved the following asymptotic lower bound on $m_r(2,q)$.

1.108 Theorem For every $\epsilon > 0$ and $\delta > 0$, there is a $q_0 = q_0(\epsilon,\delta)$ such that for every $r > q^{1/2+\delta}$, $m_r(2,q) \ge (1-\epsilon)rq$ when $q > q_0$.

1.109 Table [17] Known upper bounds on $m_r(2,q)$.

r	Conditions	$m_r(2,q) \leq$
r		$(r-1)q+r$
r	q odd	$(r-1)q+r-2$
r	q odd, $r\|q$	$(r-1)q+r/2$
r	$4 \leq r < q,\ r \not\| q$	$(r-1)q+r-3$
r	$9 \leq r < q,\ r \not\| q$	$(r-1)q+r-4$
r	q prime, $r \geq (q+3)/2$	$(r-1)q+r-(q+1)/2$
r	$r \leq 2q/3$	$(r-1)q+q-r$
r	$r \geq q/2,\ (r,q)>1,\ K$ has a skew line	$(r-1)q+q-r$
r	$r > 2q/3$	$(r-1)q+(q+r-r/q)/2-$ $\sqrt{(q+r-r/q)^2/4-(r^2-r)}$
r	no skew line to K	$rq-\sqrt{(q+1-r)q}$
r	no skew line to K	$m_r(2,q) \leq (r-1)q+\lfloor r^2/q \rfloor$
r	no skew line to K, $\sqrt{q}\|r$	$m_r(2,q) < (r-1)q+\lfloor r^2/q \rfloor$
r	$(r,q)=1,\ r<\sqrt{q}+1$	$(r-1)q+1$
r	$(r,q)=1;\ 6 \leq r \leq \sqrt{2q}+1 \leq q-1$	$(r-1)q+1$
r	$(r,q)=p^e,\ K$ has a skew line	$(r-1)q+p^e$
r	q prime, $r \leq (q+1)/2$	$(r-1)q+1$

1.110 Table [1] The known exact values and known intervals for $m_r(2,q)$, q small.

$r \backslash q$	3	4	5	7	8	9	11	13	16	17	19
2	4	6	6	8	10	10	12	14	18	18	20
3		9	11	15	15	17	21	23	$28-33$	$28-35$	$31-39$
4			16	22	28	28	$32-34$	$38-40$	52	$48-52$	$52-58$
5				29	33	37	$43-45$	$49-53$	65	$61-69$	$68-77$
6				36	42	48	56	$64-66$	$78-82$	$78-86$	$86-96$
7					49	55	67	79	$93-97$	$94-103$	$105-115$
8						65	$77-78$	92	120	$114-120$	$124-134$
9							$89-90$	105	$128-131$	137	$147-153$
10							$100-102$	$118-119$	$142-148$	154	172
11								$132-133$	$159-164$	$166-171$	191
12								$145-147$	$180-181$	$182-189$	$204-210$
13									$195-199$	$204-207$	$225-230$
14									$210-214$	$221-225$	$242-250$
15									231	$239-243$	$262-270$
16										$256-261$	$285-290$
17											$305-310$
18											$324-330$

1.111 Remark Maximal arcs are used to construct partial geometries (see §IV.**??**).

Reference to section on partial geometries

1.11 Caps

1.112 Definition A *k-cap* in $\mathrm{PG}(d,q)$ is a set of k points, no three collinear. A k-cap of $\mathrm{PG}(d,q)$ is called *complete* when this k-cap is not contained in a $(k+1)$-cap of $\mathrm{PG}(d,q)$.

1.113 Remark In $\mathrm{PG}(2,q)$, the definitions of k-caps and of k-arcs coincide.

1.114 Definition The maximal size of a cap in $\mathrm{PG}(d,q)$ is denoted by $m_2(d,q)$ and the size of the second largest complete cap in $\mathrm{PG}(d,q)$ is denoted by $m_2'(d,q)$.

1.115 Table [17] The known exact values for $m_2(d,q)$, $d \geq 3$.

q	d	$m_2(d,q)$	q	d	$m_2(d,q)$	q	d	$m_2(d,q)$
q odd	3	q^2+1	$q=2$	d	2^d	$q=3$	5	56
q even, $q>2$	3	q^2+1	$q=3$	4	20	$q=4$	4	41

1.116 Definition A (q^2+1)-*cap* in $\mathrm{PG}(3,q)$, $q>2$, is an *ovoid* of $\mathrm{PG}(3,q)$.

1.117 Examples The elliptic quadrics in $\mathrm{PG}(3,q)$, $q>2$, and the *Tits ovoids* in $\mathrm{PG}(2,2^{2e+1})$, $e \geq 1$, are the known examples of ovoids. An elliptic quadric in $\mathrm{PG}(3,q)$ is a quadric having a quadratic equation equivalent to $f(X_0,X_1)+X_2X_3=0$, where $f(X_0,X_1)$ is a homogeneous irreducible quadratic polynomial over $\mathbb{F}_q$.

The Tits ovoids are ovoids in $\mathrm{PG}(3,2^{2e+1})$, $e \geq 1$, projectively equivalent to $K = \{(0:1:0:0)\} \cup \{(1:z:y:x) | z = xy + x^{\sigma+2} + y^{\sigma},\ \text{with } (x,y) \in \mathbb{F}_q^2 \text{ and } \sigma = 2^{e+1}\}$. Tits ovoids are not projectively equivalent to elliptic quadrics.

1.118 Theorem In $\mathrm{PG}(2,4)$ and in $\mathrm{PG}(2,16)$, every ovoid is an elliptic quadric. In $\mathrm{PG}(2,8)$ and in $\mathrm{PG}(2,32)$, every ovoid is an elliptic quadric or a Tits ovoid.

1.119 Table [17] Exact and upper bounds on $m_2'(d,q)$. The type of the $m_2(d,q)$-cap in $\mathrm{PG}(d,q)$ to which a k-cap of $\mathrm{PG}(d,q)$, with $k > m_2'(d,q)$, can be extended is given in the third column. Here, p is a prime.

d	q	$m_2'(d,q)$	$m_2(d,q)$-cap
3	q even, $q \geq 8$	$\leq q^2-q+5$	ovoid
3	3	$=8$	elliptic quadric
3	4	$=14$	elliptic quadric
3	5	$=20$	elliptic quadric
3	7	$=32$	elliptic quadric
4	3	$=19$	20-cap
5	3	$=48$	56-cap
d	2	$=2^{d-1}+2^{d-3}$	complement of a hyperplane

q odd, $q \geq 17$	$m_2'(3,q) <$	$m_2(3,q)$-cap
$q=p^{2e},\ p>2,\ e\geq 1$	$q^2-q^{3/2}/4+39q/64+O(q^{1/2})$	elliptic quadric
$q=p^{2e+1},\ p>2,\ e\geq 1$	$q^2-p^{3e+2}/4+119p^{2e+2}/64-O(p^{e+2})$	elliptic quadric
q prime, $q>2$	$2641q^2/2700-4q/135+94/27$	elliptic quadric
$q=p^h,\ p\geq 5$	$q^2-q^{3/2}/2+67q/16-O(q^{1/2})$	elliptic quadric
$q\geq 23^2,\ q=p^h,\ p\geq 3$, h even for $p=3,\ q\neq 5^5,\ 3^6$	$q^2-q^{3/2}/2+35q/16+O(q^{1/2})$	elliptic quadric

references for Tables 113 − 120 added

1.120 Theorem (Davydov and Tombak) In $\mathrm{PG}(d,2)$, $d \geq 3$, a complete k-cap K, with $d \geq 2^{d-1}+1$, has order $k = 2^{d-1}+2^{d-1-g}$ for some $g = 0,2,3,\ldots,d-1$. For each $g = 0,2,3,\ldots,d-1$, there exists a complete $(2^{d-1}+2^{d-1-g})$-cap in $\mathrm{PG}(d,2)$.

1.121 Table [17] The known upper bounds on $m_2(4,q)$.

$q = p^h,\ p$ prime	$m_2(4, q)$
q even, $q \geq 8$	$\leq q^3 - q^2 + 6q - 3$
$q = p^{2e},\ p > 2,\ e \geq 1,\ q \geq 49$	$< q^3 - q^{5/2}/4 + 39q^2/64 + O(q^{3/2})$
$q = p^{2e+1},\ p > 2,\ e \geq 1$	$< q^3 - p^{e+1}q^2/4 + 119pq^2/64 - O(p^{e+2}q)$
q prime, $q \geq 37$	$< 2641q^3/2700 - 79q^2/2700 + O(q)$
$q = p^h,\ p \geq 5,\ q \geq 19$	$< q^3 - q^{5/2}/2 + 67q^2/16 - O(q^{3/2})$
$q \geq 23^2,\ q = p^h,\ p \geq 3,$ h even for $p = 3,\ q \neq 5^5,\ 3^6$	$< q^3 - q^{5/2}/2 + 35q^2/16 + O(q^{3/2})$

1.122 Table [17] The known upper bounds on $m_2(d, q)$.

$q = p^h,\ p$ prime	$m_2(d, q)$
q even, $q \geq 16$	$m_2(5, q) < q^4 - q^3 + 5q^2 + 3q - 1$
q even, $q \geq 16,\ d \geq 6$	$< q^{d-1} - q^{d-2} + 5q^{d-3} + 2q^{d-4} + O(q^{d-5})$
$q = p^{2e},\ e \geq 1,\ q \geq 49$	$< q^{d-1} - q^{d-3/2}/4 + 39q^{d-2}/64 + O(q^{d-5/2})$
$q = p^{2e+1},\ e \geq 1$	$< q^{d-4}(q^3 - p^{e+1}q^2/4 + 119pq^2/64 - O(p^{e+2}q))$
q prime, $q \geq 37$	$< 2641q^{d-1}/2700 - 79q^{d-2}/2700 + O(q^{d-3})$
$q = p^h,\ p \geq 5,\ q \geq 19$	$< q^{d-1} - q^{d-3/2}/2 + 67q^{d-2}/16 - O(q^{d-5/2})$
$q \geq 23^2,\ q = p^h,\ p \geq 3,$ h even for $p = 3,\ q \neq 5^5,\ 3^6$	$< q^{d-1} - q^{d-3/2}/2 + 35q^{d-2}/16 + O(q^{d-5/2})$
$q > 3,\ d \geq 3$	$q^d \cdot (d+1)/(d^2) + q^{d-1} \cdot 3 \cdot d/(2(d-1)^2)$

1.123 Table [17] The known lower bounds on $m_2(d, q)$, for small d.

q	d	$m_2(d, q) \geq$	q	d	$m_2(d, q) \geq$
q even, $q > 4$	4	$2q^2 + q + 9$	$q \equiv 7 \pmod 8$	4	$(5q^2 - 4q - 9)/2$
$q \equiv 1 \pmod 8$	4	$(5q^2 - 2q - 7)/2$	q odd	5	$q^3 + q^2 + 3q + 3$
$3 < q \equiv 3 \pmod 8$	4	$(5q^2 - 8q - 13)/2$	q even	5	$q^3 + 2q^2 + q + 2$
$q \equiv 5 \pmod 8$	4	$(5q^2 - 6q - 11)/2$	q	6	$q^4 + 2q^2$

q	d	$m_2(d, q) \geq$	Condition
$q > 4$	7	$aq^4 + bq^3 + cq^2 + 1$	$m_2(4, q) \geq aq^2 + bq + c$
q odd	8	$q^5 + q^4 + 3q^3 + 3q^2 + 1$	
q even	8	$q^5 + 2q^4 + 2q^3 + 4q^2 + q + 2$	
q	9	$q^6 + 2q^4 + q^2$	

1.124 Table [17] The known lower bounds on $m_2(d, q)$, for large values of d.

q	d	$m_2(d, q) \geq$
3	$6l + v,$ $v = 7, \ldots, 12$	$112^l m_2(v, 3)$
3	$6l$	$32^l((3l/8)(7/2)^{l-1} + 1)$
> 3	$6l$	$q^{4l} + (1+l)q^{4l-2} + (l^2 - 2l + 1)q^{4l-4}$
> 3	$6l + 1$	$aq^{4l} + bq^{4l-1} + (c - a + al)q^{4l-2} + (bl - l)q^{4l-3}$
> 3	$6l + 2$	$aq^{4l+1} + bq^{4l} + (c - a + al)q^{4l-1} + (d - b + bl)q^{4l-2}$
> 3	$6l + 3$	$q^{4l+2} + (l+1)q^{4l} + (l^2 - 2l + 3)q^{4l-2}/2$
> 3	$6l + 4$	$aq^{4l+2} + bq^{4l+1} + (al + c)q^{4l} + blq^{4l-1}$
> 3	$6l + 5$	$aq^{4l+3} + bq^{4l+2} + (c + al)q^{4l+1} + (d + bl)q^{4l}$

Where for $q > 3$, the formulas for $d = 1 + 6l$ and $d = 4 + 6l$ start from $m_2(4, q) \geq aq^2 + bq + c$, the one for $d = 2 + 6l$ from $m_2(8, q) \geq aq^5 + bq^4 + cq^3 + dq^2 + eq + f$, and the one for $d = 5 + 6l$ from $m_2(5, q) \geq aq^3 + bq^2 + cq + d$. For exact values of the parameters a, b, c, d, e, f, see Table 1.123. In the first formula for $q = 3$, the corresponding lower bounds on $m_2(v, 3)$ can be found in Table 1.125.

row added to table

1.125 Table [17] The sizes of the largest known caps in PG(d, q), for $d \geq 4$ and q small.

$d\backslash q$	3	4	5	7	8	9	11	13
4	20	41	66	132	208	212	316	388
5	56	126	186	434	695	840		
6	112	288	675	2499	4224	6723		
7	248	756	1715	6472	13520	17220		
8	532	2110	4700	21555	45174	68070		
9	1216	4938	17124	122500	270400	544644		
10	2744	15423	43876	323318	878800	1411830		
11	6464	34566	120740	1067080	2812160	5580100		
12	13312							

1.12 Unitals

1.126 Definition A *unital* is a 2-$(n^3+1, n+1, 1)$ design, i.e., a geometry with n^3+1 points, $n+1$ points on each line such that any two distinct points are on exactly one line.

1.127 Remark Here the interest is not in abstract unitals (§I.**??**, Theorem ??), but in unitals embedded in a projective plane of order $q = n^2$. The classical examples of unitals are obtained as follows.

Reference to Section on Steiner systems, Theorem 4.6 (4) in first volume

1.128 Construction Let $P = \mathrm{PG}(2, q^2)$ be represented using homogeneous coordinates. Then the points $(x : y : z)$ for which $xx^q + yy^q + zz^q = 0$ form a unital. This unital is a *hermitian curve.*

1.129 Construction An other very important class of unitals are the *Buekenhout-Metz unitals.*

First, a description of the plane. Let $P = \mathrm{PG}(4, q)$ be the 4-dimensional projective space of order q and let H be a hyperplane of P. Let S be a spread of lines of H. Then the geometry $A(S)$ has as points those in $P\backslash H$ and as lines the planes of P that intersect H just in an element of S. Then $A(S)$ is an affine plane of order q^2 (Theorem 1.170). If the spread is regular, then $A(S)$ is desarguesian. Now fix a line $s \in S$ and consider a point $Q \in s$.

Then consider an ovoid O in a 3-dimensional space π_3 not through Q such that $H \cap \pi_3$ is the tangent plane to O in π_3 in the point $s \cap \pi_3$. Let U be the set of points, not in H, of the cone U with vertex Q and base O, together with the point at infinity of $A(S)$ corresponding to s. Then U is a unital in the projective closure of $A(S)$. If $A(S)$ is desarguesian one can choose O in such a way that U is not a hermitian curve.

New theorem

1.130 Theorem (Penttila and Royle) In PG$(2, 9)$, every unital is a Buekenhout-Metz unital.

1.13 Blocking Sets

1.131 Definition Let P be a projective plane. A *blocking set* is a set B of points of P such that any line contains at least one point of B and at least one point outside B. A blocking set B in PG$(2, q)$ is called *small* when $|B| < 3(q+1)/2$.

1.132 Proposition Any projective plane P of order $q \neq 2$ contains a blocking set.

1.133 Definition A blocking set B is *minimal* if through any point Q of B there is a line only intersecting B in Q.

1.134 Examples Baer subplanes and unitals in projective planes of square order are classical examples of minimal blocking sets.

1.135 Theorem (Bruen, Bruen and Thas) Let B be a minimal blocking set in a projective plane of order q. Then $q+\sqrt{q}+1 \leq |B| \leq q\sqrt{q}+1$, with $|B| = q+\sqrt{q}+1$ if and only if B is a Baer subplane and with $|B| = q\sqrt{q}+1$ if and only if B is a unital.

1.136 Theorem (Sziklai and Szőnyi) Let B be a small minimal blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$. Then every line intersects B in 1 (mod p) points. The maximal integer e for which every line intersects B in 1 (mod p^e) points is a divisor of h.

1.137 Theorem Let B be a blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$. Then

1. If $h = 0$, then $|B| \geq p + (p+3)/2$.
2. If h is even, then $|B| \geq q + \sqrt{q} + 1$.
3. If $h > 1$ is odd, then $|B| \geq q + p^e\lceil \frac{q/p^e+1}{p^e+1} \rceil + 1$, where $e < h$ is the largest divisor of h.

These bounds are sharp when $h = 1$, h even, or $h \equiv 0 \pmod 3$ with h odd.

1.138 Definition Let P be a projective plane. A *t-fold blocking set* is a set B of points of P such that any line contains at least t points of B. A t-fold blocking set B in $\mathrm{PG}(2,q)$ is called *small* when $|B| < tq + (q+3)/2$.

1.139 Remark The complement of a t-fold blocking set B in a projective plane of order q is a $\{k'; q+1-t\}$-arc K, with $k' = q^2+q+1-|B|$. Due to this correspondence, t-fold blocking sets are mainly studied for small values of t. For large values of t, instead of studying the t-fold blocking set, the complementary $\{k'; q+1-t\}$-arc is studied. New remark

1.140 Theorem (Blokhuis, Lovász, Storme and Szőnyi) Let B be a small minimal t-fold blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, $h \geq 1$. Then every line of $\mathrm{PG}(2,q)$ intersects B in t (mod p) points.

1.141 Example In $\mathrm{PG}(2,q)$, q square, it is possible to construct t-fold blocking sets by taking the union of t pairwise disjoint Baer subplanes.

1.142 Table [17] Lower bounds on the cardinalities of t-fold blocking sets in $\mathrm{PG}(2,q)$.

$q = p^h$, p prime	t	$\|B\| \geq$	Sharp
$q = p$ prime, $p > 3$	$t < p/2$	$(2t+1)(p+1)/2$	for $t = 1, (p-1)/2$
$q = p$ prime, $p > 3$	$t > p/2$	$(t+1)p$	for $t = (p+1)/2$

q	t	Condition	$\|B\| \geq$
q	t	B does not contain a line	$tq + \sqrt{tq} + 1$
q	t	B contains a line and $(t-1,q) = 1$	$q(t+1)$
q	t	B contains a line and $(t-1,q) > 1$, $t \leq q/2+1$	$tq + q - t + 2$
q	t	B contains a line and $(t-1,q) > 1$, $t \geq q/2+1$	$t(q+1)$

references added

1.143 Table [17] Lower bounds on the cardinalities of minimal t-fold blocking sets of $\mathrm{PG}(2,q)$ and characterization results. The first two columns give the conditions on q, t and k. The last two columns give the structure of B, plus an implied lower bound on the value k. Here, p prime, $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ if $p > 3$.

q	$t,\ k = \|B\| - t(q+1)$	implies k	B
p^{2d+1}	$1 \le t < q/2 - c_p q^{2/3}/2$	$\ge c_p q^{2/3}$	
$p^{2d} > 4$	$1 \le t < c_p q^{1/6},\ k < c_p q^{2/3}$	$\ge t\sqrt{q}$	union of t disjoint Baer subplanes
p^2	$1 \le t < q^{1/4}/2,\ k < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}}\rceil$	$\ge t\sqrt{q}$	union of t disjoint Baer subplanes

q	$t,\ k = \|B\| - t(q+1),$ other conditions	implies k	remark
p^{6m}	$2 \le t < p^{3m/2}/4,\ k < p^{4m}\sqrt{p}/2$ no Baer subplane in B	$\ge tp^{4m} - 4t^2p^{2m}$	
p^{6m+1}	$2 \le t < \frac{p^{3m/2+1/4}}{4},\ k < p^{4m+1} - 2p^{2m+1}$	$\ge \max(tp^{4m} - 4t^2p^{2m-1}, p^{4m+1} - p^{4m} - p^{2m+1}/2)$	$m \ge 1$
p^{6m+2}	$2 \le t < p^3/(4(p+1))$ if $m=1$ $2 \le t < p^{(3m+1)/2}/4$ if $m>1$ $k < p^{4m+2}/2$, no Baer subplane in B	$\ge tp^{4m+1} - 4t^2p^{2m}$	$m \ge 1$ $p \ge 5$
p^{6m+3}	$2 \le t < p^{(6m+3)/4}/4,\ k < p^{4m+2}\sqrt{p}/2$	$\ge tp^{4m+2} - 4t^2p^{2m+1}$	$p \ge 23$ ($m=0$) $p \ge 3$ ($m=1$)
p^{6m+4}	$2 \le t < p^{(3m+2)/2}/4,\ k < p^{4m+3} - 2p^{2m+2}$ no Baer subplane in B	$\ge \max(tp^{4m+2} - 4t^2p^{2m}, p^{4m+3} - p^{4m+2} - p^{2m+2}/2)$	$m \ge 1$
p^{6m+5}	$k < p^{4m+4}/2,\ 2 \le t < p^{3m/2+5/4}/4$ for $m>0$ $2 \le t \le (p-3)/4$ for $m=0$	$\ge \max(tp^{4m+3} - 4t^2p^{2m+1}, p^{4m+3}\sqrt{p} - p^{4m+3} - p^{2m+2}/2)$	$p \ge 5$

q	$t,\ k = \|B\| - t(q+1),$ other conditions	B
p^{6m}	$2 \le t < p^{3m/2}/4,\ k < \min(p^{4m}\sqrt{p}/2, 2p^{4m} + (t-2)p^{3m} - 16p^{2m})$	$t-1$ disjoint Baer subplanes union a t-th minimal blocking set
p^{6m+2}	$m \ge 1,\ 2 \le t < p^{3m/2+1/2}/4,\ k < \min(p^{4m+2}/2, 2p^{4m+1} + (t-2)p^{3m+1} - 16p^{2m})$	union of t disjoint Baer subplanes
p^{6m+4}	$2 \le t < p^{(3m+2)/2}/4,\ k < \min(p^{4m+3} - 2p^{2m+2}, (t-2)p^{3m+2} + \max(2p^{4m+2} - 16p^{2m}, p^{4m+3} - p^{4m+2} - p^{2m+2}/2))$	union of t disjoint Baer subplanes

1.144 Theorem (Bose and Burton) Let B be a set of points in $\mathrm{PG}(d,q)$. If any subspace of dimension $d-t$ has at least one point in common with B, then $|B| \ge q^t + \cdots + q + 1$ with equality if and only if B is a t-dimensional subspace.

1.145 Definition A *t-blocking set* B in $\mathrm{PG}(d,q)$ is a set of points such that any $(d-t)$-dimensional subspace contains a point of B and no t-dimensional subspace is contained in B. A t-blocking set B in $\mathrm{PG}(d,q)$ is called *minimal* when every point Q of B belongs to at least one $(d-t)$-dimensional space only intersecting B in Q.

New theorem **1.146 Theorem** (Szőnyi and Weiner) Let B be a minimal t-blocking set B of $\mathrm{PG}(d,q)$, $q = p^h$, $p > 2$ prime, and assume that $|B| < 3(q^t+1)/2$. Then any subspace that intersects B intersects it in 1 (mod p) points.

1.147 Theorem (Beutelspacher, Heim) Let B be a t-blocking set in $\mathrm{PG}(d,q)$. Then $|B| \ge q^t + \cdots + 1 + q^{t-1}\epsilon$, with $q + \epsilon + 1$ the size of the smallest blocking set in $\mathrm{PG}(2,q)$, and with equality if and only if B is the point set of a cone over a minimal blocking set of size $q + \epsilon + 1$ in $\mathrm{PG}(2,q)$.

1.148 Theorem (Bokler) The minimal t-blocking sets of cardinality at most $q^t + \cdots + q + 1 + \sqrt{q}(q^{t-1} + \cdots + q + 1)$ in $\mathrm{PG}(d,q)$, q square, $q \ge 16$, are cones with an m-dimensional vertex $\mathrm{PG}(m,q)$ and base a Baer subgeometry $\mathrm{PG}(2(t-m-1), \sqrt{q})$, for some m with $\max\{-1, 2t-d-1\} \le m \le t-1$.

1.14 Nondesarguesian Planes

1.149 Remark The projective planes $\mathrm{PG}(2,q)$ are the classical examples of finite projective planes. Many other examples of finite projective planes exist. The projective planes

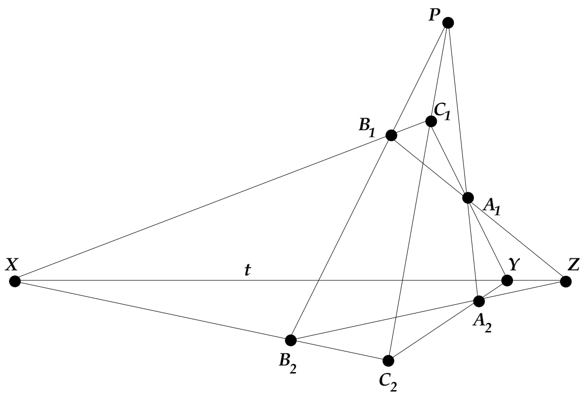
PG$(2,q)$ are also called the *desarguesian* planes since they are the only finite projective planes in which the theorem of Desargues is valid (Theorem 1.152).

1.150 Definition The *Desargues configuration* is a symmetric (10_3) configuration consisting of two triangles with vertices A_i, B_i, C_i and opposite sides a_i, b_i, c_i, $i = 1, 2$, such that the lines A_1A_2, B_1B_2, C_1C_2 are concurrent at a point P (the triangles are *in perspective* from P) and the points a_1a_2, b_1b_2, c_1c_2 are collinear on a line ℓ (the triangles are *in perspective* from ℓ). (If P is on ℓ, then the configuration is the *little Desargues configuration* and is not a (10_3).) (See §IV.**??** for more on configurations.)

Reference to section on configurations

1.151 Example The Desargues configuration.

put in desargues config



1.152 Theorem (Theorem of Desargues) In PG$(2,q)$, if two triangles with vertices A_i, B_i, C_i and opposite sides a_i, b_i, c_i, $i = 1, 2$, are in perspective from a point P, then the corresponding intersection points a_1a_2, b_1b_2, c_1c_2 are collinear on a line ℓ.

1.153 Theorem If in a finite projective plane of order q, for every two triangles with vertices A_i, B_i, C_i and opposite sides a_i, b_i, c_i, $i = 1, 2$, which are in perspective from a point P, the corresponding intersection points a_1a_2, b_1b_2, c_1c_2 are collinear on a line ℓ, then this projective plane is equal to PG$(2,q)$.

1.154 Remark The preceding theorem explains why the finite projective planes, different from PG$(2,q)$, are called *nondesarguesian* planes.

1.155 Theorem (Ostrom) Any finite projective plane of order $n \geq 5$ contains a pair of triangles which are in perspective from a point and a line.

1.156 Definition A projective plane is *pappian* if the Pappus configuration occurs for any pair of distinct lines ℓ, ℓ'. That is, given any distinct A, B, C on ℓ and any distinct A', B', C' on ℓ', the points $AB' \cap A'B$, $AC' \cap A'C$, $BC' \cap B'C$ are collinear. See Example IV.**??**.

Reference to Pappus configuration in section on configurations

1.157 Theorem Every pappian plane (finite or infinite) is desarguesian. Conversely, in the finite case (following from Wedderburn's theorem that every finite skew field is a field), every desarguesian plane is pappian.

1.158 Definition For any projective plane π, its *dual plane* π^* is defined as the plane whose points are the lines of π and whose lines are the points of π.

1.159 Remark Some projective planes are isomorphic to their dual plane. For instance, the dual plane of PG$(2,q)$ is again isomorphic to PG$(2,q)$. However, not all projective planes are isomorphic to their dual plane.

1.160 Remark If $\alpha \neq 1$ is a collineation of a projective plane π, and α fixes all lines through a point P and all points on a line ℓ, then α is called a (P,ℓ)-*perspectivity*. In particular, a (P,ℓ)-*homology* if $P \notin \ell$ and a (P,ℓ)-*elation* if P is on ℓ. The point P is the *center* and ℓ is the *axis* of the perspectivity. For a given pair (P,ℓ), the (P,ℓ)-perspectivities of π form a subgroup, denoted by $\Sigma_{(P,\ell)}$, of Aut π.

1.161 Definition π is (P,ℓ)-*transitive* if for any distinct points A, B not on ℓ and collinear with $P\,(A \neq P \neq B)$ there is a (P,ℓ)-perspectivity α in Aut π such that $A^\alpha = B$.

1.162 Proposition If π has order n, then

1. π is (P,ℓ)-transitive for P on ℓ if and only if $|\Sigma_{(P,\ell)}| = n$.
2. π is (P,ℓ)-transitive for P not on ℓ if and only if $|\Sigma_{(P,\ell)}| = n - 1$.

1.163 Proposition Let α be a (P,ℓ)-perspectivity of π. If Δ is a triangle having no vertex or side fixed by α, then Δ and Δ^α are in perspective from both P and ℓ.

1.164 Definition A projective plane π is (P,ℓ)-*desarguesian* if for each pair of nondegenerate triangles $\Delta_i\ (i = 1, 2)$ with vertices A_i, B_i, C_i and opposite sides a_i, b_i, c_i, such that: (1) Δ_1 and Δ_2 are in perspective from P, and (2) $X = a_1a_2$ and $Y = b_1b_2$ are on the line ℓ, then the point $Z = c_1c_2$ is on ℓ.

1.165 Theorem (Baer) A projective plane π is (P,ℓ)-transitive if and only if it is (P,ℓ)-desarguesian.

1.166 Remark The preceding theorem is a particular example that properties of the automorphism group of a projective plane sometimes are equivalent to geometric properties of this plane.

Let π be a projective plane of order $n \geq 5$ and G the collineation group of π. Define $T(G) = \{(P,\ell)|G \text{ is } (P,\ell)\text{-transitive}\}$. The projective planes can be classified by looking at all possibilities for $T(G)$. This provides the *Lenz-Barlotti classification* of projective planes [8]. However, projective planes can also be classified according to the coordinatizing algebra as the properties of such an algebra translate the geometric properties of the plane as well as those of its collineation group. This is presented in the next section.

1.167 Definition π is (m,ℓ)-*transitive* if it is (P,ℓ)-transitive for all points P on m; dually, π is (P,Q)-*transitive* if it is (P,ℓ)-transitive for all lines ℓ on Q. If π is (ℓ,ℓ)-transitive for some line ℓ, then ℓ is a *translation line* of π and π is a *translation plane* with respect to ℓ. A *translation point* for π is a point P such that π is (P,P)-transitive; then π is a *dual translation plane* with respect to P.

1.168 Remark If π is a translation plane with respect to a line ℓ, then usually $\pi^\ell = \pi \setminus \ell$ is also called a *translation plane*. The translation plane is considered as an affine plane, its line at infinity being the translation line. Also, the translation group of such an affine plane is the group of all (ℓ,ℓ)-elations, and acts transitively on the points of the affine plane.

1.169 Remark t-Spreads in $\mathrm{PG}(2t+1,q)$ (See §1.8) are equivalent to translation planes. Let $P = \mathrm{PG}(2t+2,q)$ and let H be a hyperplane of P. Let S be a t-spread of H. Then define the geometry $A(S)$ with points those of $P \setminus H$, and lines the $(t+1)$-dimensional subspaces of P that intersect H precisely in an element of S.

1.170 Theorem (André) $A(S)$ is a translation plane of order q^{t+1}. Conversely, for any translation plane A, there is an integer t so that a t-spread S in $H = \mathrm{PG}(2t+1,q)$ exists for which $A = A(S)$. In addition, $A(S)$ is desarguesian if and only if S is regular.

1.171 Definition A projective plane in which every line is a translation line is a *Moufang plane.*

1.172 Proposition Finite Moufang planes are desarguesian.

1.15 Coordinatization of Arbitrary Projective Planes

1.173 Construction Let π be a projective plane of order n and R a set of n symbols with two distinguished symbols 0 and 1, $0 \neq 1$. We coordinatize π by the set $R \cup \{\infty\}$ where ∞ is a symbol not in R, with respect to a given quadrangle.

Let P, X, Y, I be a quadrangle in π, and consider the lines $\ell_\infty = XY$, $\ell_1 = PY$, $\ell_2 = PX$ and the points $A = XI \cap \ell_1$, $B = YI \cap \ell_2$, $J = AB \cap \ell_\infty$. Assign the elements of R to the points on $\ell_1 \setminus \{Y\}$ in an arbitrary bijective manner except that 0 is assigned to P and 1 to A. If $c \in R$ is assigned to the point $C \in \ell_1$, write $(0, c)$ for C. Next, if $D \in \ell_2 \setminus \{X\}$, consider $D' = JD \cap \ell_1$; if D' is $(0, d)$, then D is $(d, 0)$. For any point H not on ℓ_∞, if $XH \cap \ell_1$ is $(0, g)$ and $YH \cap \ell_2$ is $(h, 0)$, then H has the coordinates (h, g). For a point $M \in \ell_\infty \setminus \{Y\}$, take the line joining M to $(1, 0) = B$, and let $(0, m)$ be the point in which it meets ℓ_1; then M is given the coordinate (m). Finally, Y has coordinate (∞).

Next, coordinatize the lines. Let ℓ be a line not on Y with (m) and $(0, k)$ the points at which it meets ℓ_∞ and ℓ_1, respectively. Then ℓ has coordinates $[m, k]$. If $\ell \neq \ell_\infty$ contains Y, then ℓ is the line $[k]$ if $\ell \cap \ell_2 = (k, 0)$. Finally, ℓ_∞ is the line $[\infty]$.

To determine via the coordinates when two elements are incident, one uses the incidences of π to define a ternary operation T on R. Namely, if $a, b, c \in R$, then $T(a, b, c) = k$ if and only if (b, c) is on $[a, k]$. Thus $(0, k)$ is the intersection of ℓ_1 with the line joining (a) to (b, c) so that, given a, b, c, the value of k is uniquely determined.

1.174 Proposition Let π be a projective plane coordinatized by a set R. If T is defined by $T(a, b, c) = k$ if and only if (b, c) is on $[a, k]$, then the following properties hold.

1. $T(a, 0, c) = T(0, b, c) = c$ for all $a, b, c \in R$.
2. $T(a, 1, 0) = T(1, a, 0) = a$ for all $a \in R$.
3. If $a, b, c, d \in R$, $a \neq c$, then there is a unique $x \in R$ such that $T(a, b, c) = T(x, c, d)$.
4. If $a, b, c \in R$, then there is a unique $x \in R$ such that $T(a, b, x) = c$.
5. If $a, b, c \in R$, $a \neq c$, then there is a unique ordered pair $x, y \in R$ such that $T(a, x, y) = b$ and $T(c, x, y) = d$.

1.175 Definition Any ternary ring (i.e. set with a ternary operation) with two distinguished elements $0, 1$ satisfying properties (1)-(5) of Proposition 1.174 is a *planar ternary ring* (PTR).

1.176 Proposition If (R, T) is a PTR, then the structure π defined as follows is a projective plane. The points of π are ordered pairs (x, y), where $x, y \in R$, together with elements of the form (x), $x \in R$, and (∞) where ∞ is a symbol not in R. Lines are given by ordered pairs $[m, k]$, $m, k \in R$, together with elements of the form $[m]$, $m \in R$, and $[\infty]$. Incidence is defined as follows:

(x, y) is on $[m, k] \iff T(m, x, y) = k$,
(x, y) is on $[k] \iff x = k$,
(x) is on $[m, k] \iff x = m$,
(x) is on $[\infty]$ for all $x \in R$ and (∞) is on $[k]$ for all $k \in R$.

Finally, (∞) is on $[\infty]$.

1.177 Remark On a PTR (R,T), for any $a,b \in R$, define $a+b = T(1,a,b)$ and for all $a,b \in R^*$, define $a \cdot b = ab = T(a,b,0)$. Then $\langle R;+\rangle$ and $\langle R^*;\cdot\rangle$ are loops with 0 and 1 the respective identities. If (R,T) is any PTR with $T(a,b,c) = ab+c$ for all $a,b,c \in R$, then (R,T) is *linear*, and the PTR is linear. A plane coordinatized by a skewfield may be coordinatized by a linear PTR.

The algebraic properties of PTRs and/or of the associated loops are linked to the groups of perspectivities admitted by the corresponding planes; in turn, these groups reflect the geometric structure of the planes. Linearity can be characterized by the validity of a suitable little Desargues configuration.

1.178 Proposition (R,T) is linear with associative addition if and only if π is $((\infty),[\infty])$-transitive.

1.179 Definition A *cartesian group* is a linear PTR (R,T) with associative addition.

1.180 Proposition A cartesian group (R,T) satisfies the left distributive law $a(b+c) = ab+ac$, for all a,b,c in R, if and only if π is $((0),[\infty])$-transitive.

1.181 Definition A *(left) quasifield* (R,T) is a cartesian group satisfying the left distributive law.

1.182 Corollary π is coordinatized by a quasifield with the line ℓ as $[\infty]$ if and only if ℓ is a translation line.

1.183 Proposition If (R,T) is a quasifield, then $\langle R;+\rangle$ is an abelian group.

1.184 Proposition (R,T) is linear with associative multiplication if and only if π is $((0),[0])$-transitive.

1.185 Proposition If (R,T) is linear, then (R,T) has associative multiplication and satisfies the left distributive law if and only if π is $((\infty),[0,0])$-transitive.

1.186 Definition A *nearfield* is a quasifield with associative multiplication.

1.187 Proposition The dual plane π^* of π can be coordinatized by dualizing the quadrangle in a natural way. Associativity of addition is preserved but the left distributive law becomes the right distributive law and yields a right quasifield.

1.188 Proposition If (R,T) is linear with associative addition then (R,T) satisfies the right distributive law if and only if π is $((\infty),[0])$-transitive.

1.189 Corollary (R,T) is a right quasifield if and only if (∞) is a translation point.

1.190 Definition A *semifield* (or *division ring*) is a (left) quasifield satisfying the right distributive law. (So, in a semifield both distributive laws hold.)

1.191 Proposition (R,T) is a semifield if and only if π is $((\infty),[\infty])$-, $((0),[\infty])$- and $((\infty),[0])$-transitive. Alternatively, (R,T) is a semifield if and only if π is a translation plane with respect to $[\infty]$ and the dual of a translation plane with respect to (∞).

1.192 Table Classification of projective planes by PTR.

PTR	Geometric Properties of π	Name
Field	(P,ℓ)-transitivity, all P and ℓ, plus configuration of Pappus	Pappian plane
Skewfield	(P,ℓ)-transitivity for all P,ℓ	Desarguesian plane
Alternative division ring	(P,ℓ)-transitivity for all incident pairs P,ℓ	Moufang plane
Semifield	(ℓ,ℓ)-transitivity and (P,P)-transitivity for one incident pair P,ℓ	Semifield plane
Nearfield	(ℓ,ℓ)-transitivity and (P,m)-transitivity $P\in\ell$, $P\notin m$	Nearfield plane
Right nearfield	(P,P)-transitivity and (Q,ℓ)-transitivity, P on ℓ, Q not on ℓ	Dual nearfield plane
Quasifield	(ℓ,ℓ)-transitivity for one ℓ	Translation plane
Right quasifield	(P,P)-transitivity for one P	Dual translation plane

1.193 Construction Given a PTR (R,T) of order n with $R=\{0,1,\ldots,n-1\}$, for any $x\in R^*$ construct an $n\times n$ matrix $\{x\}$ as follows: the entry of $\{x\}$ in position (i,j) is $T(x,i,j)$. Then $\{x\}$ is a latin square and $\{x\}$ is orthogonal to $\{y\}$ if $x\neq y$. This yields a complete set of $n-1$ MOLS. Conversely, given such a set of MOLS in normal form, $A_1,A_2,\ldots,A_{n-1}$, where A_1 has $(0,\,1,\ldots,n-1)^t$ as its first column, label the squares $\{x\}$ so that $\{x\}$ is the square with x in the $(1,0)$-position, $x=1,2,\ldots,n-1$. Defining $T(x,i,j)=(i,j)$-th entry in $\{x\}$, and $T(0,i,j)=j$, for all i,j, yields a PTR (R,T).

1.194 Proposition There exists a finite projective plane of order n if and only if there exists a complete set of $n-1$ MOLS of order n (see §II.**??** and §II.**??**).

Reference to latins squares and MOLS section

1.16 Hall and André Planes

1.195 Definition A *quasifield* Q is an algebra with two binary operations $+$ and $\cdot$ such that

1. $\langle Q;+\rangle$ is an abelian group;
2. $\langle Q^*;\cdot\rangle$ is a loop;
3. $x(y+z)=xy+xz$ for all x,y,z in Q;
4. $0x=0$ for all $x\in Q$;
5. $ax=bx+c$ has a unique solution for x, given $a,b,c\in Q$, $a\neq b$.

1.196 Definition The *Hall quasifields*, which coordinatize the Hall planes, are defined as follows. Let F be a field and $f(s)=s^2-as-b$ an irreducible quadratic polynomial over F. Let H be a two dimensional right vector space over F with basis elements 1 and λ so that $H=\{x+\lambda y|x,y\in F\}$. Take as addition in H the addition of the vector space and define a multiplication as follows: if $y=0$, $x(z+\lambda t)=xz+\lambda(xt)$; if $y\neq 0$, $(x+\lambda y)(z+\lambda t)=xz-y^{-1}tf(x)+\lambda(yz-xt+at)$. Then $\langle H;+,\cdot\rangle$ is a Hall quasifield.

1.197 Proposition A Hall quasifield H is associative (i.e. is a nearfield) if and only if $F=\mathbb{F}_2$ (in which case $H=\mathbb{F}_4$) or $F=\mathbb{F}_3$ and $f(s)=s^2+1$.

1.198 Remark The Hall quasifield of order 9 (in fact, a nearfield) can also be defined as follows. Let F be $\mathbb{F}_9$ and define a new multiplication $\circ$ on F by $x\circ y=xy$ if x is a square and $x\circ y=xy^3$ if x is not a square. Then $\langle F;+,\circ\rangle$ is a quasifield; moreover, multiplication is associative. If $F=\mathbb{F}_{q^2}$, q an odd prime power, and a multiplication

$\circ$ is defined by $x \circ y = xy$ if x is a square, and $x \circ y = xy^q$ if x is not a square, then $\langle F; +, \circ\rangle$ is a quasifield, actually a nearfield.

1.199 Remark The Hall planes are translation planes, so can be defined by a t-spread in $\mathrm{PG}(2t+1, q)$ (Theorem 1.170). If one replaces one 1-regulus of a regular 1-spread in $\mathrm{PG}(3, q)$, one obtains a 1-spread that is not regular. It are precisely these 1-spreads in $\mathrm{PG}(3, q)$ which define the Hall planes.

1.200 Construction Assume $F = \mathbb{F}_{q^m}$, $K = \mathbb{F}_q$ and $\mathcal{G} = \mathrm{Aut}_K(F)$ so that $\mathcal{G}$ is the cyclic group of order m and K is the subfield of F fixed by $\mathcal{G}$. The *norm function* over K of F is

$$N_{F/K} : F \to K : \alpha \mapsto N_{F/K}(\alpha) = \alpha^{(q^m-1)/(q-1)},$$

and maps F onto K. Let φ be any mapping from K into $\mathcal{G}$ that maps the identity 1 of K^* onto the identity of $\mathcal{G}$. A quasifield F_φ can then be defined. The elements of F_φ are the elements of F, addition is the same and multiplication $\circ$ is defined by

$$0 \circ y = 0 \text{ for all } y \in F, \quad x \circ y = xy^{\alpha_x} \text{ for all } x, y \in F,\ x \neq 0,$$

where $\alpha_x \in \mathcal{G}$ is the automorphism of F given by $N_{F/K}(x)^\varphi$. Then $\langle F_\varphi; +, \circ\rangle$ is an *André quasifield*. If φ is a homomorphism from K^* into $\mathcal{G}$, then the André quasifield is associative. It is an *André nearfield*.

1.201 Definition A plane coordinatized by an André quasifield is an *André plane*.

1.17 Semifields

1.202 Definition A *(finite) semifield* $\mathcal{S}$ is an algebra $\langle S; +, \cdot\rangle$ such that

1. $\langle S; +\rangle$ is an abelian group with identity 0;
2. $\langle S^*; \cdot\rangle$ is a loop with identity 1;
3. both left and right distributive laws hold: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ for all $a, b, c \in S$.

1.203 Proposition A proper semifield (i.e. one which is not a (skew)-field) contains three elements a, b, c such that $(ab)c \neq a(bc)$.

1.204 Theorem A finite proper semifield has order p^n, p a prime, $n \geq 3$ an integer, and $p^n \geq 16$.

1.205 Definition For a semifield $\mathcal{S}$, define the

left nucleus of $\mathcal{S}$: $N_l = \{x \in S | x(ab) = (xa)b \text{ for all } a, b \in S\}$;
right nucleus of $\mathcal{S}$: $N_r = \{x \in S | (ab)x = a(bx) \text{ for all } a, b \in S\}$;
middle nucleus of $\mathcal{S}$: $N_m = \{x \in S | (ax)b = a(xb) \text{ for all } a, b \in S\}$.

The intersection of these three nuclei (they are sometimes called the *semi-nuclei*) is the *nucleus* N of S.

1.206 Remarks When S is finite of characteristic p, N contains $\mathbb{F}_p$. All nuclei are (skew)-fields and obviously, S is a left (right) vector space over N_l, (N_r), N_m, and N.

1.207 Example Let $F = \mathbb{F}_4 = \{0, 1, \omega, \omega^2 = 1 + \omega\}$ be the field of four elements. The elements of the semifield V have the form $u + \lambda v$, $u, v \in F$, λ a symbol not in F. Addition is defined componentwise, whereas multiplication is defined as follows:

$$(u + \lambda v)(x + \lambda y) = (ux + v^2 y) + \lambda(vx + u^2 y + v^2 y^2).$$

The nucleus of V is $\mathbb{F}_2$. (In V, $(ab)c = a(bc)$ if any two of a, b, c are in $\mathbb{F}_4$.) V has six automorphisms σ_{ij}, $i = 0, 1, 2$, $j = 1, 2$, such that $(u + \lambda v)^{\sigma_{ij}} = u^j + \lambda\omega^i v^j$ and an anti-automorphism $\tau : (u + \lambda v)^\tau = u + \lambda v^2$. The plane coordinatized by V is a translation plane and a dual translation plane of order 16, namely the so-called semifield plane with kern $\mathbb{F}_2$, *Semi2*.

1.208 Example The following semifield W has the same elements and the same addition as V in Example 1.207, but multiplication is defined as follows:

$$(u + \lambda v)(x + \lambda y) = (ux + \omega v^2 y) + \lambda(vx + u^2 y).$$

In W the associative law holds whenever one of a, b, c is in F. The nucleus of W is $\mathbb{F}_4$. The plane coordinatized by W is a translation plane and a dual translation plane and is the so-called semifield plane of order 16 with kern $\mathbb{F}_4$, *Semi4*. The semifields in this and Example 1.207 are essentially the only semifields of order 16.

1.209 Example *Dickson commutative semifields.* Assume $F = \mathbb{F}_{p^m}$, p odd, $m > 1$, σ a nontrivial automorphism of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and f a nonsquare in F. Then the Dickson semifield has elements $a+\lambda b$, $a, b \in F$, λ a symbol not in F, addition is componentwise and multiplication is defined as follows:

$$(a + \lambda b)(c + \lambda d) = (ac + b^\sigma d^\sigma f) + \lambda(ad + bc).$$

The planes coordinatized by the Dickson semifields have many interesting properties; e.g. they admit polarities, their full collineation groups are solvable.

1.210 Example *Albert's twisted fields.* Define a new multiplication on $F = \mathbb{F}_{p^n}$ by

$$x \circ y = xy^q - cx^q y,$$

where $q = p^m$, $1 \le m < n$ and $c \ne a^{q-1}$ for any $a \in \mathbb{F}_{p^n}$. Then $\langle F; +, \circ\rangle$ is a pre-semifield, i.e. $\langle F^*; \circ\rangle$ is a quasigroup but not a loop. Take any $b \in F^*$ and define a new multiplication $*$ by

$$(x \circ b) * (b \circ y) = x \circ y;$$

then $\langle F; +, *\rangle$ is a semifield with multiplicative identity $b \circ b$.

1.18 The Hughes Planes

1.211 Remark Hughes planes are nondesarguesian planes of order q^2, q an odd prime power, which cannot be coordinatized by any linear PTR. They can be constructed by the nearfield $\langle N; +, \circ\rangle$, where $N = \mathbb{F}_{q^2}$, $+$ is addition in the field and the multiplication $\circ$ is defined by

$$x \circ y = \begin{cases} xy & \text{if } x \text{ is a square in } \mathbb{F}_{q^2}, \\ xy^q & \text{if } x \text{ is not a square in } \mathbb{F}_{q^2}. \end{cases}$$

The kernel of this nearfield N is the field $F = \mathbb{F}_q$ and every element of F commutes with each element of N.

1.212 Construction To construct the Hughes plane $Hu(q^2)$ of order q^2, consider the set $V = \{(x, y, z)|x, y, z \in N\}$. Define addition $+$ on V componentwise and define a left scalar multiplication by the elements of N by $k \circ (x, y, z) = (k \circ x, k \circ y, k \circ z)$. Both the points and the lines of $Hu(q^2)$ are the elements of $N^3 \setminus \{(0, 0, 0)\}$, and (x, y, z) represents $\{(k \circ x, k \circ y, k \circ z)|k \in N^*\}$. The points of $Hu(q^2)$ can be identified with the points of $\mathrm{PG}(2, q^2)$. To define the incidence, fix a basis $\{1, t\}$ for N as a vector space over F. To determine whether (x, y, z) is incident with (u, v, w), express $u = a + ta_1$, $v = b + tb_1$, $w = c + tc_1$. Then (u, v, w) and (x, y, z) are incident if $xa + yb + zc + (xa_1 + yb_1 + zc_1) \circ t = 0$. The set π_0 of all points (x, y, z) such that

$x, y, z \in F$, together with the lines joining them, forms a desarguesian Baer subplane of $Hu(q^2)$ which is left invariant by the full collineation group of $Hu(q^2)$ and is also called the *real Baer subplane.* This full collineation group depends on q^2; namely,

If $q^2 = 3^2$, then Aut $Hu(9) = PGL(3,3) \times Sym_3$.
If $q^2 = p^2$, $p > 3$, then Aut $Hu(p^2) = PGL(3,p) \times C_2$.
If $q^2 = p^{2m}$, then Aut $Hu(q^2) = PGL(3,p^m) \rtimes C_{2m}$.

1.213 Proposition $Hu(q^2)$ is not (P, ℓ)-transitive for any choice of P and ℓ, and hence is neither a translation plane nor a dual translation plane.

1.214 Remarks $Hu(q^2)$ is a *semitranslation plane*, which means the following. Let ℓ_0 be any line of π_0 (i.e. ℓ_0 is a line of $Hu(q^2)$ such that $\pi_0 \cap \ell_0$ is a line of π_0), then $Hu(q^2)$ admits all elations with axis ℓ_0 and center a point on $\pi_0 \cap \ell_0$ which fix π_0.

1.19 The Figueroa Planes

1.215 Remark The *Figueroa* planes form an infinite class of nondesarguesian planes of order q^3, q a prime power, which are neither translation nor semitranslation planes.

1.216 Construction The desarguesian plane $\mathrm{PG}(2, q^3)$ over $\mathbb{F}_{q^3}$ admits a planar collineation α of order 3 ($\langle\alpha\rangle = \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^3})$). Then the points and lines of $\mathrm{PG}(2, q^3)$ fall into three disjoint classes. For a point P,

$$P \text{ is of } \begin{cases} \text{type I} & \text{if } P^\alpha = P, \\ \text{type II} & \text{if } P, P^\alpha, P^{\alpha^2} \text{ are collinear and distinct,} \\ \text{type III} & \text{if } P, P^\alpha, P^{\alpha^2} \text{ are not collinear.} \end{cases}$$

Line types are defined dually. Define as follows an involutory bijection μ between the points of type III and the lines of type III. For a point P and a line ℓ both of type III, $P^\mu = P^\alpha P^{\alpha^2}$ and $\ell^\mu = \ell^\alpha \cap \ell^{\alpha^2}$. Let $\mathcal{P}$ be the set of points and $\mathcal{L}$ the set of lines of $\mathrm{PG}(2, q^3)$. Define a new incidence structure $Fig(q^3) = (\mathcal{P}, \mathcal{L}, \mathrm{I}_F)$ in terms of the incidence I of $\mathrm{PG}(2, q^3)$:

$$P \,\mathrm{I}_F\, \ell \iff \begin{cases} P^\mu \,\mathrm{I}\, \ell^\mu & \text{if } P \text{ and } \ell \text{ are both of type III} \\ P \,\mathrm{I}\, \ell & \text{otherwise;} \end{cases}$$

then $Fig(q^3)$ is the *Figueroa plane* of order q^3 [12].

1.217 Proposition For $q > 2$, the Figueroa plane is not desarguesian. The points and lines of type I form a desarguesian subplane of order q of both $\mathrm{PG}(2, q^3)$ and $Fig(q^3)$, and if $\mathcal{A}$ denotes its collineation group, then the collineation group of $Fig(q^3)$ is $\langle\alpha\rangle \rtimes \mathcal{A}$.

1.20 Derivation

1.218 Remark *Derivation* is a construction due to Ostrom which for $q > 2$ produces a new (nonisomorphic) plane of order q^2 from a given one of the same order.

1.219 Construction Assume π is a plane of square order q^2, and ℓ_∞ is a line of π containing a set Δ of $q+1$ points with the following property: *there exist $q^2(q+1)$ Baer subplanes of π all of which contain Δ such that any two of them either share the points in Δ only or share also one point in π^{ℓ_∞}*. Then a new affine plane $\pi^{\mathcal{D}} \setminus \ell_\infty$, the *derived* plane of π^{ℓ_∞} with respect to Δ, can be constructed:

1. the points of $\pi^{\mathcal{D}} \setminus \ell_\infty$ are the points of π^{ℓ_∞};
2. all lines of π^{ℓ_∞} which, in π, meet $\ell_\infty \setminus \Delta$ are lines of $\pi^{\mathcal{D}} \setminus \ell_\infty$;

3. each line of π^{ℓ_∞} which, in π, meets ℓ_∞ at a point of Δ is substituted by one of the Baer subplanes described above;
4. incidence is set theoretic inclusion.

This new affine plane uniquely completes to a projective plane, the *derived plane* of π with respect to Δ.

1.220 Remarks Derivation can also be discussed from an algebraic point of view (see [20]). By deriving the derived plane of π with respect to the same Δ, π is recovered. Not all planes are derivable. The desarguesian planes are derivable with respect to any line and any Δ. By deriving $\mathrm{PG}(2, q^2)$, one obtains the Hall plane of order q^2. Both the semifield planes of order 16 are derivable. All Hughes planes are derivable when ℓ_∞ is a line of the real Baer subplane π_0 and $\Delta = \pi_0 \cap \ell_\infty$.

The four planes of order 9 form a chain in the following sense:

$$\mathrm{PG}(2,9) \overset{\text{derive}}{\rightsquigarrow} \mathrm{Hall}(9) \overset{\text{dualize}}{\rightsquigarrow} \mathrm{Hall}(9)^* \overset{\text{derive}}{\rightsquigarrow} Hu(9),$$

and the arrows can be reversed.

1.21 Projective Planes of Small Order

1.221 Table [11, 27] The number of distinct examples of particular substructures in the four planes of order nine.

	$\mathrm{PG}(2,9)$	Hall(9)	Hall(9)*	$Hu(9)$
Ovals	1	1	1	2
Maximal {21;3}-arcs	0	0	0	0
Unitals	2	4	4	8

1.222 Table [5, 9, 10, 24] The number of distinct translation planes of small order q.

$q=2$	$q=3$	$q=4$	$q=5$	$q=7$	$q=8$
1	1	1	1	1	1
$q=9$	$q=16$	$q=25$	$q=27$	$q=32$	$q=49$
2	8	21	7	≥ 9	1347

1.223 Remarks The two translation planes of order nine are $\mathrm{PG}(2,9)$ and Hall(9).

The eight translation planes of order sixteen are: (1) $\mathrm{PG}(2,16)$, (2) the semifield plane *SEMI2* with kernel $\mathbb{F}_2$, (3) the semifield plane *SEMI4* with kernel $\mathbb{F}_4$, (4) the Hall plane Hall(16), (5) the Lorimer-Rahilly plane LMRH, (6) the Johnson-Walker plane JOWK, (7) the derived semifield plane DSFP, and (8) the Dempwolff plane DEMP [10].

The seven translation planes of order 27 are: (1) $\mathrm{PG}(2,27)$, (2) a generalized twisted field plane, (3) a Hering plane, (4) a flag transitive plane, (5) a Sherk plane, (6) a second flag transitive plane, and (7) an André plane [9].

Mathon found by an exhaustive computer search that there are at least nine translation planes of order 32 defined by a 4-spread in $\mathrm{PG}(9,2)$ having a non-trivial stabilizer group.

1.224 Remark Twenty-two planes of order 16 are known. There are the eight translation planes, mentioned in Remark 1.223. The first three of the planes from Remark 1.223 are self-dual; the remaining five planes have duals HALL(16)*, LMRH*, JOWK*, DSFP*, and DEMP* which not are translation planes. There are four known semi-translation planes of order 16: BBH1, BBH2, JOHN, and BBS4. The plane BBH1 is self-dual; the other three semitranslation planes have dual planes BBH2*, JOHN* and

BBS4* which have not yet arisen. The two remaining planes MATH and MATH* are the other two known planes of order 16 [28].

1.225 Table [28] The number of distinct hyperovals in the known planes of order 16. The name of every plane is followed by the number of distinct hyperovals.

$PG(2,16)$	2	SEMI2	17	SEMI4	3	HALL	4	HALL*	3	LMRH	6
LMRH*	1	JOWK	6	JOWK*	1	DSFP	22	DSFP*	0	DEMP	15
DEMP*	2	BBH1	3	BBH2	2	BBH2*	0	JOHN	1	JOHN*	0
BBS4	1	BBS4*	0	MATH	1	MATH*	3				

formulation changed

1.226 Remarks It is particularly interesting to note that the planes DSFP*, BBH2*, JOHN*, and BBS4* do not contain any hyperovals. Also, since the external lines to a hyperoval in a plane of order 16 define a maximal $\{120;8\}$-arc in the dual plane, using Remark 1.224 where the relation between the planes and their dual planes is described, from Table 1.225 also the number of distinct maximal $\{120;8\}$-arcs in the planes of order 16 can be deduced.

1.22 Substructures in Nondesarguesian Planes

1.227 Remark A great deal of research has also been done on substructures in nondesarguesian projective planes. The following list gives examples of such substructures.

1. Translation planes of order q^2 with kernel of order q have unitals [3].
2. Translation planes of order q^t, $t \geq 2$, with kernel of order q have blocking sets of size in the interval $[q^t + q^{t-1} + 1, q^t + q^{t-1} + \cdots + q + 1]$ [2].
3. Hall(q^2) has unitals [3], blocking sets [2], hyperovals if $q \geq 4$, q even [26], and ovals if q is odd [21].
4. *Hu*(q^2) has unitals [30] and ovals [29].
5. *Fig*(q^3) has unitals if q is a square, hyperovals if $q > 2$ even [6], and ovals if q is odd [4].
6. Thas proved that certain translation planes of order 2^{2m} contain maximal $\{2^{3m} - 2^{2m} + 2^m; 2^m\}$-arcs [32]. Hamilton and Quinn constructed maximal arcs in symplectic translation planes [14].

Some of these are *inherited substructures* from $PG(2,q)$. Let π be an arbitrary projective plane of order q. Then π can sometimes be looked at as a modification of $PG(2,q)$. The points of π can be identified with those of $PG(2,q)$ and the lines of π can be regarded as point sets of $PG(2,q)$. An oval in $PG(2,q)$ can sometimes remain to be an oval in π. In which case this oval in π is an *inherited* oval of $PG(2,q)$.

1.228 Remark Of course, differences between the results on substructures in desarguesian planes and on substructures in nondesarguesian planes appear, some of which are very surprising. In particular observe the non-existence of hyperovals in four of the known planes of order 16 (Table 1.225). Other examples include the following.

1. Menichetti proved: In Hall(q^2), q even, there exist complete q^2-arcs [25]. Segre, for q odd, and Tallini, for q even, proved that complete q-arcs do not exist in $PG(2,q)$.
2. In $PG(2,q)$, q odd, there exist (complete) $(q+1)$-arcs and in $PG(2,q)$, q even, there exist (complete) $(q+2)$-arcs. The existence is known of complete $(q - \sqrt{q}+1)$-arcs in $PG(2,q)$, $q > 4$ square (Theorem 1.88). But all the other known infinite classes of complete k-arcs in $PG(2,q)$ have size at most $(q+1)/2 + \sqrt{q}$. In particular, there exist complete k-arcs, with $(q+1)/2 - \sqrt{q} \leq k \leq (q+1)/2 +$

$\sqrt{q}$, consisting of half of the points of elliptic cubic curves in PG$(2,q)$. So, an important problem in PG$(2,q)$ is that of the existence of complete k-arcs, with $(q+1)/2+\sqrt{q} < k < q-\sqrt{q}+1$.

By contrast, in certain André planes of order $q = s^2$, complete k-arcs having size in this interval have been constructed by Szőnyi [31]. Let $k|(s-1)$, then there exist in certain of these André planes complete k-arcs of size $((m-1)(q-1)/m + O(q^{1/2}))$-arcs, where $m = k$ if k is odd, and where $m = k/2$ if k is even.

3. It is known that the only subplanes of PG$(2,q)$, $q = p^h$, p prime, $h \geq 1$, are the subplanes PG$(2,p^e)$, $e|h$ (Remark 1.51). In particular, the subplanes of PG$(2,q)$ have the same characteristic as PG$(2,q)$. This is no longer always the case for nondesarguesian planes. De Resmini and Leone proved that the derived Hughes plane of order 25 contains desarguesian subplanes PG$(2,q)$, for $q = 2,3$ and $q = 5$ [7].

1.23 See Also

check section labels

§I.??	Affine and projective spaces, together with specific substructures, give Steiner systems.
§I.??	Projective planes are symmetric designs.
§I.??	Affine planes are resolvable designs.
§III.??, §III.??	Finite geometries provide constructions for PBDs.
§III.??, §III.??	Links with linear spaces.
§III.??, §III.??	Related incidence structures: generalized quadrangles and partial geometries.
§IV.??	Hall triple systems generalize affine planes.
[15, 16, 17, 19]	Standard references and survey article on finite geometry.
[8, 20, 22]	Standard references on projective planes.

References

[1] S. Ball and J. W. P. Hirschfeld, *Bounds on (n,r)-arcs and their application to linear codes*, Finite Fields Appl., 11 (2005), pp. 326–336. [cited on pages]

[2] A. E. Brouwer and H. A. Wilbrink, *Blocking sets in translation planes*, J. Geom., 19 (1982), p. 200. [cited on pages]

[3] F. Buekenhout, *Existence of unitals in finite translation planes of order q^2 with a kernel of order q*, Geom. Dedicata, 5 (1976), pp. 189–194. [cited on pages]

[4] W. E. Cherowitzo, *Ovals in Figueroa planes*, J. Geom., 37 (1990), pp. 84–86. [cited on pages]

[5] T. Czerwinski and D. Oakden, *The translation planes of order twenty-five*, J. Combin. Theory Ser. A, 59 (1992), pp. 193–217. [cited on pages]

[6] M. J. de Resmini and N. Hamilton, *Hyperovals and unitals in Figueroa planes*, European J. Combin., 19 (1998), pp. 215–220. [cited on pages]

[7] M. J. de Resmini and A. O. Leone, *Subplanes of the derived Hughes plane of order 25*, Simon Stevin, 67 (1993), pp. 289–322. [cited on pages]

[8] P. Dembowski, *Finite Geometries*, Springer-Verlag, 1968. [cited on pages]

[9] U. Dempwolff, *Translation planes of order 27*, Des. Codes Cryptogr., 4 (1994), pp. 105–121. [cited on pages]

[10] U. Dempwolff and A. Reifart, *The classification of the translation planes of order 16 I*, Geom. Dedicata, 15 (1983), pp. 137–153. [cited on pages]

[11] R. H. F. Denniston, *On arcs in projective planes of order 9*, Manuscripta Math., 4 (1971), pp. 61–89. [cited on pages]

[12] T. Grundhöfer, *A synthetic construction of the Figueroa planes*, J. Geom., 26 (1986), pp. 191–201. [cited on pages]

[13] N. Hamilton and R. Mathon, *On the spectrum of non-Denniston maximal arcs in* $PG(2, 2^h)$, European J. Combin., 25 (2004), pp. 415–421. [cited on pages]
[14] N. Hamilton and C. T. Quinn, *m-Systems of polar spaces and maximal arcs in projective planes*, Bull. Belg. Math. Soc. Simon Stevin, 7 (2000), pp. 237–248. [cited on pages]
[15] J. W. P. Hirschfeld, *Finite Projective Spaces Of Three Dimensions*, The Clarendon Press, Oxford University Press, 1985. [cited on pages]
[16] ———, *Projective Geometries Over Finite Fields. Second Edition*, The Clarendon Press, Oxford University Press, 1998. [cited on pages]
[17] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, in Finite Geometries, Dev. Math., 3, Kluwer Acad. Publ., 2001, pp. 201–246. [cited on pages]
[18] J. W. P. Hirschfeld and T. Szőnyi, *Constructions of large arcs and blocking sets in finite planes*, European J. Combin., 12 (1991), pp. 499–511. [cited on pages]
[19] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, The Clarendon Press, Oxford University Press, 1991. [cited on pages]
[20] D. R. Hughes and F. C. Piper, *Projective Planes*, Springer-Verlag, 1973. [cited on pages]
[21] G. Korchmáros, *Ovali nei piani di Hall di ordine dispari*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8), 56 (1974), pp. 315–317. [cited on pages]
[22] H. Lüneburg, *Translation planes*, Springer-Verlag, Berlin, 1980. [cited on pages]
[23] R. Mathon, *New maximal arcs in Desarguesian planes*, J. Combin. Theory Ser. A, 97 (2002), pp. 353–368. [cited on pages]
[24] R. Mathon and G. F. Royle, *The translation planes of order* 49, Des. Codes Cryptogr., 5 (1995), pp. 57–72. [cited on pages]
[25] G. Menichetti, *q-Archi completi nei piani di Hall di ordine* $q = 2^k$, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8), 56 (1974), pp. 518–525. [cited on pages]
[26] C. M. O'Keefe, A. A. Pascasio, and T. Penttila, *Hyperovals in Hall planes*, European J. Combin., 13 (1992), pp. 195–199. [cited on pages]
[27] T. Penttila and G. F. Royle, *Sets of type* (m, n) *in the affine and projective planes of order nine*, Des. Codes Cryptogr., 6 (1995), pp. 229–245. [cited on pages]
[28] T. Penttila, G. F. Royle, and M. K. Simpson, *Hyperovals in the known projective planes of order* 16, J. Combin. Des., 4 (1996), pp. 59–65. [cited on pages]
[29] T. G. Room, *Polarities and ovals in the Hughes plane*, J. Austral. Math. Soc., 13 (1972), pp. 196–204. [cited on pages]
[30] L. A. Rosati, *Unitals in Hughes planes*, Geom. Dedicata, 27 (1988), pp. 295–299. [cited on pages]
[31] T. Szőnyi, *Complete arcs in non-Desarguesian planes*, Ars Combin., 25 (1988), pp. 169–178. [cited on pages]
[32] J. A. Thas, *Construction of maximal arcs and partial geometries*, Geom. Dedicata, 3 (1974), pp. 61–64. [cited on pages]