JOURNAL OF COMBINATORIAL THEORY, Series A 49, 26–66 (1988)

Rings of Geometries II

DAVID G. GLYNN*

ANSTO, Lucas Heights Research Laboratories, Locked Bag No. 1, Menai, NSW 2234, Australia

Communicated by the Managing Editors

Received December 20, 1986

Linear spaces are investigated using the general theory of "Rings of Geometries I." By defining geometries and ring structures in several different ways, formulae for linear spaces embedded in finite projective and affine planes are obtained. Several "fundamental theorems" of counting in finite projective planes are proved which show why configurations with at least three points per line and at least three lines through every point are important. These theorems are illustrated by finding the formulae for the number of k-arcs in a projective plane of order q for all $k \leqslant 8$ and also by finding a formula for the number of blocking sets. A quick proof that a projective plane of order 6 does not exist follows from the formula for the number of 7-arcs in such a plane. © 1988 Academic Press, Inc.

INTRODUCTION

This paper is a continuation of "Rings of Geometries I" and needs to be read with a knowledge of the theory and notation introduced in that paper [10]. Section numbers starting with 1 or 2 refer to that paper. We are interested here in the combinatorial theory of finite projective and affine planes. This involves setting up various closed sets of "geometries" (see Definitions 1.4 and 2.1) and investigating the inclusion numbers associated with these. We noted after Theorem 2.6 that the investigation of inclusion numbers is equivalent to the investigation of the coefficients of the natural ring of the set of geometries. While following this course of action, we shall also see that in the case of subconfigurations of projective planes there is at least one other "geometrically defined" ring which is of use in the calculations—the coefficients of this ring are easier to calculate than those of the natural ring and are related by formulae to the latter. Closely related to the definition of these new rings is the idea of imposing partial orders other than the "natural one" (see Notation 1.7). Of course, these new partial orders are "geometrically defined."

In Section 3 we define the relevant classes of geometries associated with the types of subconfigurations of projective planes that we intend to

* Present address: Department of Mathematics, University of Canterbury, Private Bag, Christchurch 1, New Zealand.

0097-3165/88 $3.00

consider and then we prove the basic theorems about calculating the coefficients of the rings. Several of these theorems are given the title "fundamental" because they appear to be a fairly substantial advance in the understanding of the combinatorics of finite planes. We give two versions of the "fundamental theorem" which correspond to two different definitions of configuration—one is based on points as elements and the other has both points and lines as elements. Section 4 contains explicit calculations based on the results of Section 3.

3. Linear Spaces and Geometries

3.1 Definition (Projective planes). A *projective plane* may be thought of as a combinatorial structure (S, α) (see Example 1.8), where S is a set of *points*, and α is a mapping from 2^S to $\{0, 1\}$ such that

(a) $A \subseteq S$, $|A| \leqslant 2 \Rightarrow A^\alpha = 1$; $A \subseteq B$, $B^\alpha = 1 \Rightarrow A^\alpha = 1$,

(b) $A \subseteq S$, $B \subseteq S$, $A^\alpha = B^\alpha = 1$, $|A \cap B| \geqslant 2 \Rightarrow (A \cup B)^\alpha = 1$,

(c) $A \subseteq S$, $B \subseteq S$, $A^\alpha = B^\alpha = 1 \Rightarrow$ there exist $C \subseteq S$, $D \subseteq S$, such that $C \supseteq A$, $D \supseteq B$, $C^\alpha = D^\alpha = 1$ and $|C \cap D| \geqslant 1$, and

(d) there exists a subset Q of 4 points of S such that $A^\alpha = 0$ for all $A \subseteq Q$ with $|A| > 2$.

If we call a subset of S that is mapped to 1 by α *collinear*, then it is easy to see that the above structure is equivalent to the standard. (See, e.g., [4], [11] or [12].) The *lines* of the projective plane are the maximal subsets that are mapped to 1. If S is finite, then it is standard theory that there is a unique integer q, called the *order* of the plane, such that $|S| = q^2 + q + 1$, each line has size $q + 1$, and there are precisely $q + 1$ lines containing each point. Now if we construct the natural geometry (see Example 1.8) from (S, α) then in general it has the following:

(i) One kind of subgeometry of size $1: L_1 = \{\cdot\}$.

(ii) One kind of subgeometry of size $2: L_2 = \{\cdot\,\cdot\}$.

(iii) Two kinds of subgeometry of size $3: L_3 = \{.\dot{}., \text{•–•–•}\}$.

(iv) Three kinds of subgeometry of size $4: L_4 = \{\because\!\cdot, \text{•–}\dot{\text{•}}\text{–•}, \text{•–•–•–•}\}$.

The investigation of the above types of subgeometries of projective planes leads us to the following class of geometries.

3.2 Definition (Linear geometries). Let $L = \mathrm{Ext}(L_4)$, where L_4 is the set of three geometries of size 4 above that can be embedded in projective planes. (See Definition 2.7 for the extension process Ext.) L is called the class of *linear geometries*.

Note that L can be identified with the class of *linear spaces* which are ordered triples (P, G, I), where P is a set of points, G is a set of lines, and I is an incidence relation between points and lines satisfying two conditions:

(a) Each line contains at least three points.

(b) Each subset of two points is incident with at most one line.

(Sometimes it is more convenient to admit the subsets of 2 non-collinear points also as lines. Then axiom (b) above becomes: every subset of 2 points is incident with a unique line. However, we shall clearly state when we assume this.)

A major part of this paper is directed towards finding formulae for the inclusion numbers of linear geometries in finite projective planes. Let the number of linear geometries on i points be l_i. Then J. Doyen [5] calculated (by hand) that the first 10 terms of the sequence $l_0, l_1, ..., l_9, ...,$ are 1, 1, 1, 2, 3, 5, 10, 24, 69, 384, ...,—the author has written a computer program which verified Doyen's calculations except for a few minor mistakes in the automorphism groups. The sequence for linear geometries with at most 3 points per line was found to be 1, 1, 1, 2, 2, 3, 5, 11, 32, 163, 1680, ..., and a consideration of the 1680 ten-point linear geometries having 0, 1, 2, ..., 13 lines of 3 points each gave the sequence 1, 1, 2, 5, 14, 32, 90, 209, 386, 460, 332, 119, 28, 2. (13 is the maximum number of 3-point-lines for a 10-point linear geometry.) Of the 332 linear geometries with 10 points and 10 lines of 3 points each, there are precisely 10 which have 3 lines through each point. These are called the 10_3 configurations—the "Desargues" configuration is one of them. There are also three 9_3, one 8_3, and one 7_3 configurations. Note that the 10_3 configurations are associated with regular graphs of valence 3 on 10 vertices as follows. Given a 10_3, define a graph with vertices as the points of the configuration and two vertices adjacent if the corresponding points of the 10_3 are not joined by a 3-point line. Then it is interesting that Desargues' 10_3 configuration is associated with the Petersen graph. Further information on 10_3 configurations can be found in [3] and [13], which are separated by more than a hundred years, but still present similar ideas!

The above paragraph should give the reader some idea of the complexity of the problem as the number of points approaches 10. See [6] for a discussion of the number of linear geometries on n points and see [18] for a good book on sequences. Questions involving linear spaces and their embeddability in finite projective planes are considered in [7].

3.3 Definition (Partial orderings). Apart from the natural partial ordering $\leqslant$ induced by the subgeometry structure of linear geometries, we shall find it useful to also have various "finer" partial orderings defined—these will be denoted by a Greek letter preceding the $\leqslant$. The ordering is first defined on models—two geometries are partially ordered if there are models for them that are partially ordered. If a and b are two linear geometries with models A and B, respectively, define

(i) $A\ \alpha\!\leqslant B$ if the set of elements S of A is a subset of the set of elements of B and every line of A is a (complete) line of B_s;

(ii) $A\ \beta\!\leqslant B$ if the set of elements of A is a subset of the set of elements of B and every triple of collinear points of A is also collinear in B.

Note that if a and b are linear geometries, then $a \leqslant b \Rightarrow a\ \alpha\!\leqslant b \Rightarrow a\ \beta\!\leqslant b$. A similar relationship holds for models of linear geometries. Thus β is "finer" than α which is "finer" than the natural partial ordering.

3.4 Definition (Inclusion and extension numbers for partial orderings). If a and b are linear geometries then the inclusion number of a in b, with respect to the partial order γ, is

$$\gamma(a, b] = |\{M \mid M\ \gamma\!\leqslant N, \bar{M} = a\}|,$$

where N is a fixed model of b.

Also, the extension number of a to b, with respect to the partial order γ, is

$$[a, b)\gamma = |\{\overline{N_B} \mid M\ \gamma\!\leqslant N, \overline{N_B} = b\}|,$$

where M is a fixed model of a, on a fixed subset of a fixed set B of size $|b|$.

Recall from Definition 1.6 that $\bar{M}$ is the geometry corresponding to the model M. Thus $\overline{N_B}$ denotes the geometry corresponding to the model N_B which is induced by the set B of elements. (The present notation of this paper has been slightly modified from that of Definition 1.6 to change B to a suffix.)

Of course, when γ is the "natural" partial order $\leqslant$, the definitions above reduce to those of Definition 1.9. It is also an easy exercise, similar to Theorem 1.10, to show that these numbers satisfy

$$[a]\ \gamma(a, b]\ n! = [a, b)\gamma\ [b], \text{ where } n = |b| - |a|.$$

Recall from Notation 1.7 that $[a]$ denotes the size of the group of automorphisms of a. Thus it is the number of permutations of the element set of a that preserve the geometrical substructure.

Also,

$$a\ \gamma\!\leqslant b \Leftrightarrow \gamma(a, b] > 0 \Leftrightarrow [a, b)\gamma > 0.$$

3.5 DEFINITION (Closed sets). A set of linear geometries D is called *γ-closed* (where γ is a partial order) if, for every pair of geometries a and b in D, we have

$$a\,\gamma\!\leqslant c\,\gamma\!\leqslant b \Rightarrow c \in D.$$

3.6 THEOREM (Converting between partial orderings). *Let a and b be linear geometries in L. If γ is a partial order finer than the natural one (e.g., α or β),*

(a) $\gamma(a, b] = \sum_c \gamma(a, c](c, b]$, *where the sum is over all c with $a\,\gamma\!\leqslant c \leqslant b$, and with $|c| = |a|$.*

(b) $(a, b] = \sum (-1)^m \gamma(a_0, a_1]\, \gamma(a_1, a_2] \cdots \gamma(a_{m-1}, a_m]\, \gamma(c, b]$, *where the sum is over all sequences $a = a_0\,\gamma\!< a_1\,\gamma\!< a_2 \cdots \gamma\!< a_m = c$, and $|a_i| = |a|$, for all i. (Thus c satisfies $a\,\gamma\!\leqslant c\,\gamma\!\leqslant b$, and $|c| = |a|$.)*

Proof. (a) Let N be a model of b. Then each model M of $a\,\gamma\!\leqslant N$ corresponds to a subset A of points of N, and there holds $M\,\gamma\!\leqslant N_A \leqslant N$. The number of models of $a\,\gamma\!\leqslant N_A$ is $\gamma(a, c]$, where $c = \overline{N_A}$, and the number of models of $c \leqslant b$ is $(c, b]$. Hence the result follows.

(b) This formula is the inverse of (a) above. It is the "Möbius inversion formula" of the partial order. For completeness we shall use matrices to get the result. Assume that $a\,\gamma\!\leqslant b$ as otherwise $(a, b] = 0$ and the right-hand side is an empty sum. Let $D_{a,b} = \{c \in L \mid a\,\gamma\!\leqslant c\,\gamma\!\leqslant b,\ |c| = |a|\} = \{d_1, ..., d_n\}$, where $|D_{a,b}| = n$ and $d_i\,\gamma\!< d_j \Rightarrow i < j$.

Define a matrix $C = (c_{ij})$, $n \times n$ over Z, by $c_{ij} = \gamma(d_i, d_j]$, for all $i, j \leqslant n$. Also define vectors e and f, both $n \times 1$ over Z, by $e_i = \gamma(d_i, b]$ and $f_i = (d_i, b]$, for all $1 \leqslant i \leqslant n$. Then, applying (a) above, there holds $e = Cf$. Now, C is an upper triangular matrix with its main diagonal consisting of all 1's. Hence $(C - I)^n = 0$. Since $f = C^{-1}e$, the inversion formula follows from the equation

$$C^{-1} = \sum_{i=0}^{n-1} (I - C)^i.$$

3.7 DEFINITION ($\langle M, N\rangle$). Let M and N be models of linear geometries on sets A and B, respectively. Then $\langle M, N\rangle$ is defined to be the model P of a linear geometry on element set $A \cup B$, that is minimal with respect to $\beta\!\leqslant$, such that $M\,\beta\!\leqslant P$ and $N\,\beta\!\leqslant P$. We call $\langle M, N\rangle$ *the model generated by M and N*. This definition is used to construct a new ring based on the set of linear geometries.

3.8 DEFINITION (The ring $D(\Gamma)$). Let Γ be a β-closed set of linear geometries. Define a ring $D(\Gamma)$ in a way similar to that of $C(\Gamma)$ in

Definition 2.3. That is, let the basis elements of the ring be $(g)_\beta$, where $g \in \Gamma$. Let the addition be the natural one and let the multiplication of basis elements be given by

$$(g)_\beta (h)_\beta = \sum_{d \in \Gamma} \beta_d^{gh} (d)_\beta,$$

where $\beta_d^{gh} = |\{(M, N) | \bar{M} = g, \bar{N} = h, \langle M, N \rangle = F\}|$, and F is a fixed model of d.

3.9 Theorem (The structure of $D(\Gamma)$). *The rings $C(\Gamma)$ and $D(\Gamma)$ are isomorphic (for Γ any β-closed set of geometries).*

Proof. First, it is possible to show that $D(\Gamma)$ is in fact a commutative ring by showing that for all $d_1, ..., d_n \in \Gamma$,

$$(d_1)_\beta \cdots (d_n)_\beta = \sum_{f \in \Gamma} \beta_f^{d_1 \cdots d_n} (f)_\beta,$$

where $\beta_f^{d_1 \cdots d_n} = |\{(M_1, ..., M_n) | \langle M_1, ..., M_n \rangle = F\}|$: the number of $M_1, ..., M_n$ that are models of $d_1, ..., d_n$, respectively, and generate a fixed model F of f. (The proof is similar to that of Theorem 2.4 and so only this outline is given.)

Now consider the map $\mu: D(\Gamma) \to C(\Gamma)$ given by

$$\sum_{d \in \Gamma} a_d (d)_\beta \to \sum_{d \in \Gamma} a_d \sum_{x \in \Gamma, |x| = |d|} \beta(d, x](x).$$

It is straightforward to show that this is an isomorphism with inverse generated by

$$(a) \to \sum_{b \in \Gamma, |b| = |a|} \sum (-1)^m \beta(a_0, a_1] \cdots \beta(a_{m-1}, a_m](b)_\beta,$$

where the second sum is as in Theorem 3.6b.

3.10 Note (The identification of $C(\Gamma)$ and $D(\Gamma)$). Since these two rings are isomorphic, we can mix the symbols (x) and $(y)_\beta$ using the equations $(d)_\beta = \sum_{x \in \Gamma, |x| = |d|} \beta(d, x](x)$ and $(a) = \sum_{b \in \Gamma, |b| = |a|} \sum (-1)^m \beta(a_0, a_1] \cdots \beta(a_{m-1}, a_m](b)_\beta$.

The homomorphism γ_g of Theorem 2.5, generated by $(d) \to (d, g]$, is also generated by $(d)_\beta \to \beta(d, g]$ and so $(d)_\beta = \sum \beta(d, g] I_g$, for all $d \in \Gamma$, where I_g is the principal idempotent of both the rings corresponding to $g \in \Gamma$.

3.11 Example (Small linear geometries—their rings and multiplication tables). Let Γ be the set of 8 linear geometries on $\leqslant 4$ points. (See

Definition 3.2.) Thus the geometries are $a=\Phi$, $b=$ a single point, $c=2$ points, $d=3$ non-collinear points, $e=3$ collinear points, $f=4$ non-collinear points, $g=3$ points on a line plus a point off that line, $h=4$ collinear points. As a check that the previous theory has been correctly understood, we present the multiplication tables for the rings $C(\Gamma)$ and $D(\Gamma)$. In these two tables $a, \ldots, h$ are short-hand for (a), ..., (h), and $A, \ldots, H$ stand for $(a)_\beta, \ldots, (h)_\beta$.

$C(\Gamma)$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	$b+2c$	$2c+3d+3e$	$3d+4f+3g$	$3e+g+4h$	$4f$	$4g$	$4h$
c	c	$2c+3d+3e$	$c+6d+6e+6f+6g+6h$	$3d+12f+9g$	$3e+3g+12h$	$6f$	$6g$	$6h$
d	d	$3d+4f+3g$	$3d+12f+9g$	$d+12f+6g$	$3g$	$4f$	$3g$	0
e	e	$3e+g+4h$	$3e+3g+12h$	$3g$	$e+12h$	0	g	$4h$
f	f	$4f$	$6f$	$4f$	0	f	0	0
g	g	$4g$	$6g$	$3g$	g	0	g	0
h	h	$4h$	$6h$	0	$4h$	0	0	h

$D(\Gamma)$	A	B	C	D	E	F	G	H
A	A	B	C	D	E	F	G	H
B	B	$B+2C$	$2C+3D$	$3D+4F$	$3E+G$	$4F$	$4G$	$4H$
C	C	$2C+3D$	$C+6D+6F$	$3D+12F$	$3E+3G$	$6F$	$6G$	$6H$
D	D	$3D+4F$	$3D+12F$	$D+12F$	$E+3G$	$4F$	$4G$	$4H$
E	E	$3E+G$	$3E+3G$	$E+3G$	$E+12H$	G	$G+12H$	$4H$
F	F	$4F$	$6F$	$4F$	G	F	G	H
G	G	$4G$	$6G$	$4G$	$G+12H$	G	$G+12H$	$4H$
H	H	$4H$	$6H$	$4H$	$4H$	H	$4H$	H

The isomorphism between $C(\Gamma)$ and $D(\Gamma)$ is given by

$$A=a;\ B=b;\ C=c;\ D=d+e;\ E=e;\ F=f+g+h;\ G=g+4h;\ H=h.$$

The principal idempotents of the rings are:

- $I_a=a-b+c-d-e+f+g+h=A-B+C-D+F$
- $I_b=b-2c+3d+3e-4f-4g-4h=B-2C+3D-4F$
- $I_c=c-3d-3e+6f+6g+6h=C-3D+6F$
- $I_d=d-4f-3g=D-E-4F+G$
- $I_e=e-g-4h=E-G$
- $I_f=f=F-G+3H$
- $I_g=g=G-4H$
- $I_h=h=H.$

Note that the multiplicative coefficients for $D(\Gamma)$ are often somewhat simpler and more easily calculated than for $C(\Gamma)$.

3.12 DEFINITION (The projective plane ring $\Pi(q)$). The *projective plane ring* $\Pi(q)$, $(q \in Z, q \geqslant 2)$, is defined to be the ring $C(L)/\mathrm{Id}(q)$, where $\mathrm{Id}(q)$ is the set of all identities of $C(L)$ that are satisfied for all linear subgeometries of projective planes of order q.

Thus $\mathrm{Id}(q)$ is the ideal of all identities

$$\sum_{a \in L} \delta_a(a) = 0,$$

where δ_a is a polynomial in q over the rationals, such that for all projective planes π of order q,

$$\sum_{a \in L} \delta_a(a, \pi] = 0.$$

The problem of combinatorics in finite projective planes is to find the above identities. For example, in $\Pi(q)$ the following hold:

- (point) = (line of $q+1$ points) $= (q^2+q+1)\, I$, where I is the identity ring element.
- (k points, no three collinear)$_\beta = \binom{q^2+q+1}{k} I$.

Sometimes we present identities holding in $\Pi(c)$, where c is an integer. This just means that we take the special case of identities holding for all projective planes of order c.

3.13 DEFINITION (Preliminaries before a proof of the fundamental theorem). If M is a model of a linear geometry g on point set A, then every extension of M to a model of a linear geometry having one more point can be defined as follows. Let S be a set of disjoint lines and/or subsets of size 2 in A not on a line. Let P be an element not in A. Now define the model $M(P, S)$ to be the model having the same lines as M not in S, and also having the lines in $\{l \cup \{P\} \mid l \in S\}$.

$g(S)$ is defined to be the linear geometry $\overline{M(P, S)}$. From now on, unless otherwise stated, a "line" of a linear geometry denotes an "ordinary" line of $\geqslant 3$ points or else a set of two points not on an ordinary line.

3.14 LEMMA (Preliminaries before a proof of the fundamental theorem). *Let g be a finite linear geometry. Let l be a line of g. Let m be a line of g skew to l (if m exists). Then in $\Pi(q)$ the following hold*:

(a) $(g(\phi))_\beta = (g, g(\phi)]^{-1} (q^2+q+1-|g|)(g)_\beta$,

(b) $(g(\{l\}))_\beta = (g, g(\{l\})]^{-1} \sum_{h\, \beta \geqslant g, |h| = |g|} \sum_k (q+1-|k'|)(h)$,

where the second sum is over all lines k of models G of g $\beta \leqslant$ a fixed model H

of h, such that $g(\{l\})=\overline{G(P,\{k\})}$ and $k \leqslant$ a line k' of H, where P is a fixed point not in H,

(c) $(g(\{l,m\})_\beta=(g,g(\{l,m\})]^{-1}\sum_{h\,\beta\geqslant g,\,|h|=|g|}\sum_{\{u,v\}}\mu_{\{u,v\}}(h)$,

where the second sum is over all sets of two skew lines $\{u,v\}$ of models G of $g\ \beta\leqslant H$ (a fixed model of h), such that $g(\{l,m\})=\overline{G(P,\{u,v\})}$, P is a fixed point not in H, and where

$$\mu_{\{u,v\}}=\begin{cases}1 & \text{if } u \text{ and } v \text{ are not on the same line in } H\\ q+1-|k| & \text{if } u \text{ and } v \text{ are on the same line } k \text{ in } H.\end{cases}$$

Proof. (a) In the ring $D(L)$,

$$\begin{aligned}&(g)_\beta\,(\cdot)_\beta=(g,g(\phi)](g(\phi))_\beta+|g|(g)_\beta\\ &\Rightarrow (g)_\beta\,\{(\cdot)_\beta-|g|I\}=(g,g(\phi)](g(\phi))_\beta\\ &\Rightarrow (g(\phi))_\beta=(g,g(\phi)]^{-1}\,(g)_\beta\,\{(\cdot)_\beta-|g|\,I\}.\end{aligned}$$

Since $(\cdot)_\beta=(q^2+q+1)\,I$ in $\Pi(q)$, the result follows.

(b) Let P be a model of a projective plane π of order q. Let $n=|\{(G,X)|\ \bar{G}=g,\ \ \bar{X}=g(\{l\}),\ \ G<X\,\beta\leqslant P\}|$. Then $n=(g,g(\{l\})]\times\beta(g(\{l\}),\pi]$. Now, given $G\,\beta\leqslant P$ with $\bar{G}=g$, G induces a unique model H of a subgeometry $h\leqslant\pi$. (Thus $G\,\beta\leqslant H\leqslant P$, and $|g|=|h|$.) Given such a model H, the number of ways of extending $G\,\beta\leqslant H$ to a model X of $g(\{l\})$ $\beta\leqslant P$ is given by the second sum. Hence

$$n=\sum_{h\,\beta\geqslant g,\,|h|=|g|}\ \sum_{k}(q+1-|k'|)(h,\pi].$$

Dividing the two values for n above by $(g,g(\{l\})]$ gives the result.

(c) Let P be a model of a projective plane π of order q. Let $r=|\{(G,Y)|\bar{G}=g,\ \bar{Y}=g(\{l,m\}),\ G<Y\,\beta\leqslant P\}|$. Then $r=(g,g(\{l,m\})]\times\beta(g(\{l,m\}),\pi]$. Now given $G\,\beta\leqslant P$ with $\bar{G}=g$, there is a unique H with G $\beta\leqslant H\leqslant P$ and $|G|=|H|$, and there are $\sum\mu_{\{u,v\}}$ extensions from G to a model Y of $g(\{l,m\})$. Thus

$$r=\sum_{h\,\beta\geqslant g,\,|h|=|g|}\ \sum_{\{u,v\}}\mu_{\{u,v\}}(h,\pi].$$

Dividing the two values of r obtained above by $(g,g(\{l,m\})]$ gives us the required result.

3.15 Definition (Variables of $\Pi(q)$). A *variable* of $\Pi(q)$ is an element (c), where $c\in L$ is a linear geometry, such that c has at least three lines of at least three points each through every point, and c is connected.

("Connected" means that if M is a model of c, it is not the union of two disjoint models $A \neq \Phi$ and $B \neq \Phi$ such that $M = \langle A, B \rangle$.)

3.16 THEOREM (The fundamental theorem). *Let g be a finite linear geometry. Then there is a formula for (g) in $\Pi(q)$ which is a polynomial in the variables (v) of $\Pi(q)$ with $|v| \leqslant |g|$, and also in q (with coefficients over the rational numbers). For $|g| \leqslant 6$, the formula has no variables, whereas for $|g| \leqslant 13$, the formula is linear in the variables.*

Proof. We now describe an algorithm which will calculate the formulae for all finite linear geometries. Let L_n be the set of linear geometries on $\leqslant n$ points. Suppose we have already calculated the formulae for (g), for all $g \in L_n$. Note that this is equivalent to the calculation of the formulae for $(g)_\beta$ by using the equation (and its inverse) from Theorem 3.6:

$$(g)_\beta = \sum_c \beta(g, c](c) \text{ in } \Pi(q), \text{ where } g\,\beta \leqslant c, \text{ and } |c| = n.$$

We calculate the formula for (h), $h \in L_{n+1} \setminus L_n$, as follows. If h is a variable then the formula is the trivial $(h) = (h)$, and so we assume that h is generated by a collection of m disjoint variables $v_1, ..., v_m$, or there is a point P of h on only 0, 1, or 2 lines of $\geqslant 3$ points each.

In the former case we have the equation

$$(v_1)_\beta \cdots (v_m)_\beta = k(h)_\beta + \sum_{d \in L_n} l_d(d)_\beta, \qquad \text{for some } k, l_d \in Z.$$

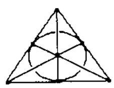
From this we have a formula for $(h)_\beta$.

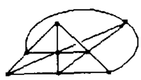
In the latter case we use Lemma 3.14 to obtain a formula for $(h)_\beta$ in terms of geometries which are $\beta \geqslant h \setminus P$ and have n points. Using the inversion formula of Theorem 3.6, as applied to β and $\Pi(q)$, gives us the result.

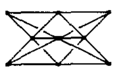
The smallest variable linear geometry is the projective plane of order 2, which has 7 points. (See Theorem 3.18.) Hence the formula for a geometry on $\leqslant 6$ points is a "constant"—that is, it is a polynomial in q, the order of the projective plane. The only way to get non-linear terms in the variables in the formulae for n-point geometries is for disjoint variables on $\leqslant n$ points to exist. Thus we see that the smallest pair of disjoint variables is made up of two disjoint projective planes of order 2, which have a union of 14 points. Hence, the formula for geometries on $\leqslant 13$ points is linear in the variables.

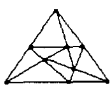
3.17 CONJECTURE (About the fundamental theorem). *If g is a finite non-variable linear geometry with p points, m lines and f flags (point/line incidences), we conjecture that the constant term for (g) in $\Pi(q)$, (i.e., a polynomial* *in q over the rationals), is of degree $2(p+m)-f$ in q. Also, the coefficient of $q^{2(p+m)-f}$ is $1/[g]$, and the constant term multiplied by $[g]$ is a polynomial in q over the integers. ($[g]$ is the size of the group of automorphisms of g.)*

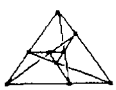
3.18 THEOREM (The variable linear geometries on 9 points or less). *Here we present a list of all the variable linear geometries v_i on $\leqslant 9$ points and the sizes $[v_i]$ of their groups of automorphisms. The list of J. Doyen [5] can be consulted for this. It has been checked by computer with a program written by the author using the techniques summarized in Example 1.17. There is one variable on 7 points, one on 8 points, and ten on 9 points. Of the 500 linear geometries on $\leqslant 9$ points, only 12 are variables*:

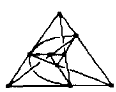
1. $[v_1] = 168$,  $= 7_3$

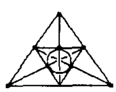
2. $[v_2] = 48$,  $= 8_3$

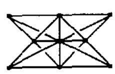
3. $[v_3] = 108$,  = "Pappus"

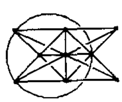
4. $[v_4] = 9$, 

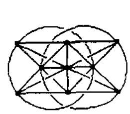
5. $[v_5] = 12$, 

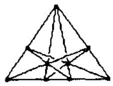
6. $[v_6] = 12$, 

7. $[v_7] = 6$, 

8. $[v_8] = 36$, 

9. $[v_9] = 36$, 

10. $[v_{10}] = 432$,  $= AG(2, 3)$

11. $[v_{11}] = 4$, 

12. $[v_{12}] = 12$, 

Note that the above configurations give the amount of "variability" in the linear subgeometries of finite projective planes with $\leqslant 9$ points.

3.19 DEFINITION (Point/line geometries). The previous "linear geometries" were based on element sets that were possible subsets of points of projective planes. Now we consider element sets based on subsets of the union of the points and the lines. Thus we define the set of *point/line geometries* (*P/L-geometries*) to be the set of those geometries g in $\mathrm{Ext}(\Gamma(0-1))$, (see Example 2.15), such that the 2×2 matrix of all 1's is not a subgeometry of g. In terms of generators, $P/L = \mathrm{Ext}(P/L_4)$, where P/L_4 is the set of 16 $(0-1)$-geometries:

- the 4×0 matrix consisting of just 4 rows,
- the four 3×1 matrices with zero, one, two and three 1's,
- the zero 2×2 matrix,
- the 2×2 matrix with a single 1,
- the 2×2 identity matrix,
- the 2×2 matrix with two 1's in a row and two 0's in the other,
- the 2×2 matrix with two 1's in a column and two 0's in the other,
- the 2×2 matrix with three 1's,
- the four 1×3 matrices with zero, one, two, and three 1's,
- the 0×4 matrix consisting of just 4 columns.

(We saw in Example 2.15 that $\mathrm{Ext}(\Gamma(0-1))$ is essentially the class of geometries induced by the matrices containing only 0's and 1's. An element set of such a geometry is the union of the sets of rows and columns of the matrix. Two geometries are considered to be equivalent if there is a bijection from rows to rows and columns to columns preserving the matrix structure.)

Note that we consider the rows to be points and the columns to be lines. In a P/L-geometry, a point is "incident" with a line if the corresponding P/L-subgeometry on 2 elements corresponding to the point and line is the 1×1 identity matrix. Then we see that the P/L-geometry of a projective plane of order q is the geometry of the $q^2+q+1 \times q^2+q+1$ incidence matrix of the plane—it has $2(q^2+q+1)$ elements.

3.20 OBSERVATION (The relationship between P/L and linear geometries). We observe that an $n \times q^2+q+1$ P/L-subgeometry of the P/L-geometry of a projective plane of order q is equivalent to an n point subgeometry of the linear geometry of the projective plane, and a $q^2+q+1 \times n$ P/L-subgeometry is equivalent to an n element subgeometry of the linear geometry of the dual projective plane. This shows how a knowledge of one type of geometry can be used to get information about the other. However, in some sense it is clear that the P/L-geometries involve "finer" substructures than do the linear geometries.

Perhaps a more important observation is that the partial order α is closely associated with the concept of P/L-geometry. Thus, if g and h are linear geometries, g having i points and j lines, h having k points and m lines, then g and h correspond to $(i \times j)$ and $(k \times m)$ P/L-geometries g' and h', respectively. (Note that these P/L-geometries do not have lines incident with less than 3 points.) Then $\alpha(g, h] = (g', h']$, and so, from Theorem 3.6 we have that

$$(g', h'] = \sum_{|x| = |g|} (g', x'](x, h]$$

and conversely

$$(g, h] = \sum_{x'} (-1)^{|x'| - |g'|} (g', x'](x', h'],$$

where the second sum is over P/L-geometries x' with the same number of points as g' but having possibly more lines (of necessarily $\geqslant 3$ points each).

Thus a simplification of Theorem 3.6b (in the case of the partial order α) is possible, because of the geometrical nature of the coefficients $\alpha(g, h]$.

3.21 THEOREM (A more powerful version of the fundamental theorem). *For any finite $m \times n$ P/L-geometry g, there is a formula for the number $(g, \pi]$ of subgeometries g in a projective plane π of order q. This formula has variables of the following type: these have at least 3 points on each line, at least 3 lines through each point, at most m points and at most n lines, (cf. Definition 3.15 and Theorem 3.16).)*

Proof. The proof is very similar to that of Theorem 3.16 which uses Lemma 3.14. The main part of the proof is to find formulae for the P/L-geometries having an element on only 0, 1, or 2 elements of the opposite type, and having at most an equal number of points and lines.

Let x be a P/L-geometry. If S is a set of skew lines of x (which may be incident with only 0, 1, or 2 points in x), then define $x(S)$ to be the

P/L-geometry obtained by adding a point to x on the intersection of the lines of S. Suppose x is of type $i \times j$. That is, it has i points and j lines. Also suppose that m is a line of x and that n is a line of x skew to m (if it exists). Let π be a general projective plane of order q. Then

(a) $(x, \pi](q^2+q+1-i) = \sum_{y \text{ type } (i+1)\times j} (x, y](y, \pi]$;

(b) $(x, \pi](q+1-|m|)[x, x(\{m\})) = \sum_y (y, \pi] \sum_P \mu_P^y$,

where the first sum is over all P/L-geometries y which have one more point than x and contain x, the second sum is over all points P of y with $x = y \backslash P$, and μ_P^y is equal to the number of lines r of x on P such that $x(\{r\}) = x(\{m\})$. $|m|$ is the number of points on m in x; and

(c) $(x, \pi][x, x(\{m, n\})) = \sum_y (y, \pi] \sum_Q \nu_Q^y$,

where the first sum is over all P/L-geometries y such that y has one more point than x and contains x, the second sum is over all points Q of y with $x = y \backslash Q$, and ν_Q^y is equal to the number of pairs of lines $\{u, v\}$ of x on Q such that $x(\{u, v\}) = x(\{m, n\})$.

Using (a), (b), and (c) above, if there is a point X of a P/L-geometry y of type $(i+1)\times j$ on 0, 1, or 2 lines of y, then there is a formula for $(y, \pi]$ in terms of $y \backslash X$ and geometries with more flags than y but also of type $(i+1)\times j$. Hence, continually using the three equations above (and their duals) we obtain a formula for y in terms of "variables" with at least 3 points on each line and at least 3 lines through each point. These P/L-geometries also have at most the same number of points and lines as y.

Coupled with Observation 3.20, this theorem can be used to obtain an alternative proof of Theorem 3.16. Since it also deals with finer subgeometries we consider it to be a "more powerful" version of the fundamental theorem.

3.22 Theorem (The variables for the point/line geometries). *Here we present a list of all the variable P/L-geometries on $\leqslant 18$ elements, because these represent, by Theorem 3.21, the amount of "variability" for small P/L-geometries in finite projective planes*:

(i) 14 *elements*: *the projective plane of order* 2, *which is* 7×7 (see 3.18, v_1).

(ii) 16 *elements*: *the affine plane of order* 3 *minus a point, which is* 8×8 (*see* 3.18, v_2).

(iii) 18 *elements*: *five* 9×9 *P/L-geometries corresponding to the linear geometries of Theorem* 3.18 *which have* 9 *points and* 9 *lines* (*see* 3.18, v_3, v_4, v_5, v_{11}, *and* v_{12}).

Note that all the above P/L-geometries are self-dual: the smallest non-self-dual variables are of size 9×10 *and* 10×9.

3.23 DEFINITION (The complete-line geometries). Now we define a new class of geometry that is useful for various problems concerning finite projective and affine planes. It is called the class of *complete line geometries of order q*, $C/L(q)$, where $q \in Z$, and $q \geqslant 2$. The idea comes from taking linear subgeometries of a projective plane of order q, but only considering the "complete" lines to be important—these are the lines with the full $q+1$ points. Thus there is a unique geometry in $C/L(q)$ of size n, for all $0 \leqslant n \leqslant q$. If $q+1 \leqslant m \leqslant 2q$, there are two $C/L(q)$-geometries on m points—those containing a complete line and those not. For $2q+1 \leqslant p \leqslant 3q-1$, there are three types of $C/L(q)$-geometry—those containing 0, 1, or 2 complete lines of $q+1$ points. Clearly, it is the dual configuration of complete lines contained in the linear geometry that is important. Hence, every $C/L(q)$-geometry can be written as $h = k.\bar{g}$, where g is a linear geometry representing the dual linear geometry of complete lines, and k is a non-negative integer giving the number of "free" points of h not on any of the complete lines of $\bar{g}$. Naturally, the total number of points of h is $c_g + k$, where c_g is the number of points on the lines of $\bar{g}$. By counting the number f_g of (point, line of $\geqslant 2$ points) flags of g in two ways we can calculate that $c_g = (q+1)|g| - f_g +$ the number of lines of $\geqslant 2$ points of g. Naturally, in an investigation of $C/L(q)$, only those linear geometries g having $c_g \leqslant q^2+q+1$ are important, as otherwise $k.\bar{g}$ cannot be embedded in a projective plane of order q.

3.24 THEOREM (Formulae for the C/L-geometries in finite projective planes). *Let π be a projective plane of order q, considered to be both a dual linear geometry $\bar{\pi}$ and a complete line geometry. "Dual" denotes the treating of the lines instead of the points as the elements of geometries. Then there are the following relationships between the inclusion numbers of the respective types of geometry. Let g be a finite linear geometry and let k be an integer satisfying $k \geqslant c_g$. Then*

(a) $\binom{q^2+q+1-c_g}{k-c_g}(\bar{g}, \bar{\pi}] = \sum_{h \geqslant g} (g, h](k - c_h \cdot \bar{h}, \pi]$;

(b) $(k - c_g \cdot \bar{g}, \pi] = \sum_{h \geqslant g} (-1)^{|h|-|g|} (g, h]\binom{q^2+q+1-c_h}{k-c_h}(\bar{h}, \bar{\pi}]$.

Proof. (a) This formula comes from counting in two ways the number of ordered pairs (M, S) of a model M of $\bar{g}$ as a submodel of a fixed model of $\bar{\pi}$ which is contained in a subset S of size k which is contained in the point set of π.

(b) This is just the inverse of the formula in (a)—one can use the properties of the idempotents of the natural ring of linear geometries (see Theorem 2.5). Thus the inverse of the matrix with (i,j)th element $(g_i, g_j]$ is the matrix with (i,j)th element $(-1)^{|g_j|-|g_i|}(g_i, g_j]$.

4. Consequences of the Fundamental Theorem

We shall now illustrate the theory of the previous chapter by giving various concrete calculations of the numbers of k-arcs and blocking sets in finite projective (and also affine planes). Note that a k-arc is a set of k points of a projective plane, no 3 collinear. A blocking set of a finite projective or affine plane is a set of points that contains no line and intersects every line of the plane. Both types of substructure have been investigated in depth before—see, for example, [11]. However, the methods we use and many of the results that we obtain here are quite new (except for the "elementary" theorem which follows).

4.1 Theorem (Formulae for k-arcs in $\Pi(q), k \leqslant 6$). *Let A_k denote the linear geometry consisting of k points, no 3 collinear. Then the number of k-arcs ($k \leqslant 6$) in a general projective plane of order q is given by the following formulae, which hold in $\Pi(q)$:*

(i) $(A_1) = (q^2+q+1)\,I.$

(ii) $(A_2) = \dfrac{1}{2}(q^2+q+1)(q^2+q)\,I.$

(iii) $(A_3) = \dfrac{1}{3!}(q^2+q+1)(q^2+q)\,q^2 I.$

(iv) $(A_4) = \dfrac{1}{4!}(q^2+q+1)(q^2+q)\,q^2(q-1)^2\,I.$

(v) $(A_5) = \dfrac{1}{5!}(q^2+q+1)(q^2+q)\,q^2(q-1)^2\,(q^2-5q+6)\,I.$

(vi) $$(A_6) = \frac{1}{6!}(q^2+q+1)(q^2+q) \times q^2(q-1)^2\,(q^2-5q+6)(q^2-9q+21)\,I.$$

Proof. Since the smallest variable for $\Pi(q)$ is the Fano plane, which has 7 points, from the "fundamental" Theorem 3.16 the value of any configuration with $\leqslant 6$ points is a constant in $\Pi(q)$. The above formulae follow from the fact that the number b_n of $(n+1)$-arcs containing a fixed n-arc in any projective plane of order q is an easily calculated constant for all $n<6$. In fact, $b_0=q^2+q+1$, $b_1=q^2+q$, $b_2=q^2$, $b_3=(q-1)^2$, $b_4=q^2-5q+6$, and $b_5=q^2-9q+21$. (See [11] for a proof of this well-known fact.)

4.2 THEOREM (Formula for 7-arcs in $\Pi(q)$). *In $\Pi(q)$:*

$$(A_7)=\frac{1}{7!}(q^2+q+1)(q+1)\,q^3(q-1)^2\,(q-3)(q-5)$$
$$\times(q^4-20q^3+148q^2-468q+498)\,I-(7_3).$$

Proof. From Theorems 3.16 and 3.18 we know that there is a formula for the number (A_7) of 7-arcs in a projective plane of order q, which is equal to a constant + a linear term in the number of Fano subplanes (7_3). We could use the algorithm of the proof of Theorem 3.16 to obtain this formula. Instead, we present here a somewhat shorter method which uses fewer configurations to obtain the result. This method uses the fact that the constants associated with the partial order α, introduced in Definition 3.3(i), are easier to calculate. (Note also the important connection with the P/L-geometries considered in Observation 3.20.) Once these constants are calculated, it is quite straightforward to convert to the natural partial order. Of course, in $\Pi(q)$, $(g)_\alpha$, where g is a linear geometry, represents the value of $\alpha(g,\pi]$, for all projective planes π of order q.

Consider a 6-arc K of a projective plane π of order q. It has 15 chords (lines intersecting it in 2 points). Let there be N_i points of $\pi\backslash K$ on i chords of K. Then the following hold (see [11] for example):

- $N_0+N_1+N_2+N_3=q^2+q-5$,
- $N_1+2N_2+3N_3=15(q-1)$, and
- $N_2+3N_3=45$.

These equations imply that $N_0=q^2-14q+55-N_3$. Let there be k_i 6-arcs of π such that $N_3=i$, (where $0\leqslant i\leqslant 15$ holds). Then, counting ordered pairs of 6-arcs contained in 7-arcs gives in $\Pi(q)$:

$$7(A_7)=\sum_{i=0}^{15}k_i(q^2-14q+55-i)\,I.$$

But

$$(A_6)=\sum_{i=0}^{15}k_iI,$$

and

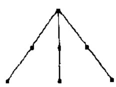
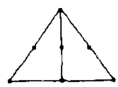
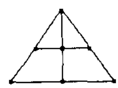
$$(c_1)=\sum_{i=1}^{15}ik_iI,$$

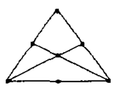
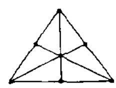
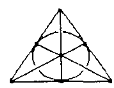
where c_1 is the linear geometry on 7 points with 3 lines of 3 points each through one of its points.

Thus, we have shown that in $\Pi(q)$:

$$7(A_7) = (q^2 - 14q + 55)(A_6) - (c_1).$$

Since (A_6) is known from Theorem 4.1(vi), we still have to calculate (c_1). We do this using the following complete list of 6 linear geometries g such that $g\,\alpha \geqslant c_1$ and $|\,g\,| = 7$.

$c_1 =$ , $c_2 =$ , $c_3 =$ ,

$c_4 =$ , $c_5 =$ , $c_6 =$  $= 7_3$.

The values of $(c_i)_\alpha$ are very easily calculated. We do it for c_1 and leave the proofs of the rest to the reader. There are $\binom{q+1}{3}$ ways of choosing three lines of π through each of the q^2+q+1 points of π. On each of these lines one can choose $\binom{q}{2}$ pairs of points. Hence

$$(c_1)_\alpha = (q^2+q+1)\binom{q+1}{3}\binom{q}{2}^3 I.$$

Let $n = (q^2+q+1)(q+1)\,q^3(q-1)^2$. Then

- $(c_1)_\alpha = (nq(q-1)^2/48)\,I$,
- $(c_2)_\alpha = (n(q-1)^2/6)\,I$,
- $(c_3)_\alpha = (n(q-2)/12)\,I$,
- $(c_4)_\alpha = (n(q-1)/8)\,I$,
- $(c_5)_\alpha = (n/24)\,I$, and
- $(c_6)_\alpha = (7_3)\,I$.

To convert the above formulae to the natural ring, we must first calculate the coefficients $x_{ij} = \alpha(c_i, c_j]$, for all $1 \leqslant (i,j) \leqslant 6$. As this is straightforward, we merely give the matrix $X = (x_{ij})$:

$$X = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 7 \\ 0 & 1 & 2 & 4 & 12 & 28 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 6 & 21 \\ 0 & 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then the inverse of X gives the coefficients needed to transfer the values of $(c_i)_\alpha$ to those of (c_i). (Note Theorem 3.6b and Observation 3.20.)

$$X^{-1}=\begin{pmatrix} 1 & -1 & 1 & 2 & -4 & 7 \\ 0 & 1 & -2 & -4 & 12 & -28 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -6 & 21 \\ 0 & 0 & 0 & 0 & 1 & -7 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We can use the first row of X^{-1} above to calculate (c_1). Thus

$$\begin{aligned}(c_1) &= (c_1)_\alpha-(c_2)_\alpha+(c_3)_\alpha+2(c_4)_\alpha-4(c_5)_\alpha+7(c_6)_\alpha \\ &= n((q(q-1)^2/48)-(q-1)^2/6+(q-2)/12+2(q-1)/8-(4/24))\,I+7(7_3) \\ &= (n/48)(q-3)^2\,(q-4)+7(7_3).\end{aligned}$$

And so,

$$(A_7)=\tfrac{1}{7}(q^2-14q+55)(A_6)-\tfrac{1}{7}(c_1).$$

This is the formula that we wanted to show, when we substitute the value of (A_6), given in Theorem 4.1(vi), and the value of (c_1) above.

4.3 Corollary (Non-Existence of $\pi(6)$). *It has been well known for a long time that there is no projective plane of order* 6. *For example, this result follows from the non-existence of two orthogonal Latin squares of order* 6, *or from the Bruck–Ryser Theorem* [2], *that no projective plane of order q exists, if $q\equiv 1$ or* 2 (mod 4) *and q is not the sum of two integral squares.*

However, we can attain a very short proof of this fact by noting that the value of $q^4-20q^3+148q^2-468q+498$ is -6 when q equals 6. Hence the number of 7-arcs plus the number of Fano subplanes in a possible plane of order 6 is negative. This is a contradiction to the fact that the number of subgeometries of a particular type in a geometry is always non-negative.

Note that it has been shown by computer-aided methods that there is no 12-arc in a putative plane of order 10 [14]. However, this result has not been used to obtain the non-existence of such a plane as yet.

4.4 Theorem (Formula for 8-arcs in $\Pi(q)$). *In $\Pi(q)$:*

$$\begin{aligned}(A_8) = \frac{1}{8!}\,&(q^2+q+1)(q+1)\,q^3(q-1)^2\,(q-5)(q^7-43q^6+788q^5-7937q^4 \\ &+47097q^3-162834q^2+299280q-222960)\,I+(8_3) \\ &-(q^2-20q+78)(7_3).\end{aligned}$$

Proof. From Theorems 3.16 and 3.18 we know that there is a formula for the number (A_8) of 8-arcs in a projective plane of order q, which is equal to a constant + a linear term in the number (7_3) of Fano subplanes + a linear term in the number (8_3) of affine planes of order 3 minus a point. We shall use a method very similar to that of the previous theorem to obtain the result.

Consider a 7-arc L of a projective plane π of order q. It has 21 chords. Let there be M_i points of $\pi\backslash L$ on i chords of L. The following hold:

- $M_0 + M_1 + M_2 + M_3 = q^2 + q - 6$,
- $M_1 + 2M_2 + 3M_3 = 21(q-1)$, and
- $M_2 + 3M_3 = 105$.

These equations imply that $M_0 = q^2 - 20q + 120 - M_3$. Let there be p_i 7-arcs of π such that $M_3 = i$ (where $0 \leqslant i \leqslant 35$ holds). Then, counting ordered pairs of 7-arcs contained in 8-arcs gives in $\Pi(q)$:

$$8(A_8) = \sum_{i=0}^{35} p_i(q^2 - 20q + 120 - i)\, I.$$

But

$$(A_7) = \sum_{i=0}^{35} p_i I,$$

and

$$(d_1) = \sum_{i=1}^{35} i p_i I,$$

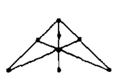
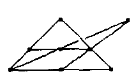
where d_1 is the linear geometry on 8 points with 3 lines of 3 points each through one of its points.

Thus we have shown that in $\Pi(q)$ there holds

$$8(A_8) = (q^2 - 20q + 120)(A_7) - (d_1).$$

Since (A_7) is known from Theorem 4.2, we still have to calculate (d_1).

Let k_i and c_j be defined as in the proof of Theorem 4.2. Let

$d_1 =$  , $d_2 =$  , $d_3 =$  .

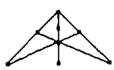
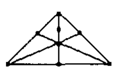
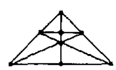
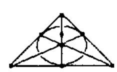
Then we have

$$\begin{aligned}(d_1) &= \sum_{i=0}^{15} i(q^2-14q+55-i)\,k_iI \\ &= (q^2-14q+55)\sum_{i=0}^{15} ik_iI - \sum_{i=0}^{15} i^2k_iI \\ &= (q^2-14q+54)\sum_{i=0}^{15} ik_iI - 2\sum_{i=0}^{15}\binom{i}{2}k_iI \\ &= (q^2-14q+54)(c_1)-2(d_2)-2(d_3).\end{aligned}$$

(By counting 6-arcs extended by two points, each on three chords, there holds $\sum_{i=0}^{15}\binom{i}{2}k_iI=(d_2)+(d_3)$.)

Hence in $\Pi(q)$ we have: $(d_1)=(q^2-14q+54)(c_1)-2(d_2)-2(d_3)$. Since (c_1) was calculated in the proof of Theorem 4.2, all we need is to calculate (d_2) and (d_3).

The complete list of linear geometries e with $|e|=8$ and $e\,\alpha\geqslant d_2$ is

$e_1=d_2=$  , $e_2=$  , $e_3=$  , $e_4=$  .

If we define the 4×4 matrix $Y=(y_{ij})$ by $y_{ij}=\alpha(e_i,e_j]$, then it is easily calculated that

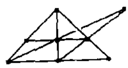
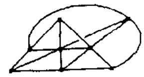
$$Y=\begin{pmatrix}1&1&1&3\\0&1&2&6\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad\text{and}\quad Y^{-1}=\begin{pmatrix}1&-1&1&3\\0&1&-2&-6\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

As in the proof of Theorem 4.2, the first row of Y^{-1} above gives the formula:

$$\begin{aligned}(d_2) &= (e_1)_\alpha-(e_2)_\alpha+(e_3)_\alpha+3(e_4)_\alpha \\ &= (q^2+q+1)\binom{q+1}{2}\binom{q}{2}^2\binom{q-1}{2}I-(q^2+q+1)\binom{q+1}{2}\binom{q}{2}^2 2(q-2)\,I \\ &\quad + [(q^2+q+1)\binom{q+1}{2}\binom{q}{2}^2 I-21(7_3)]+3[7(q-2)(7_3)] \\ &= \tfrac{1}{2}(q^2+q+1)\binom{q+1}{2}\binom{q}{2}^2[(q-1)(q-2)-4(q-2)+2]\,I+21(q-3)(7_3) \\ &= (n/16)(q-3)(q-4)\,I+21(q-3)(7_3),\end{aligned}$$

where n is as in the proof of Theorem 4.2.

The complete list of linear geometries f with $|f| = 8$ and $f\alpha \geqslant d_3$ is

$f_1 = d_3 =$  $, f_2 =$  $, f_3 =$  $= (8_3)$.

If we define the 3×3 matrix $Z = (z_{ij})$ by $z_{ij} = \alpha(f_i, f_j]$, then it is easily calculated that

$$Z = \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & 8 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{and} \quad Z^{-1} = \begin{pmatrix} 1 & -1 & 4 \\ 0 & 1 & -8 \\ 0 & 0 & 1 \end{pmatrix}.$$

As above the first row of Z^{-1} gives the formula:

$$\begin{aligned}(d_3) &= (f_1)_\alpha - (f_2)_\alpha + 4(f_3)_\alpha \\ &= \binom{q^2+q+1}{2}\binom{q}{3}^2 6I - \tfrac{1}{6}(q^2+q+1)(q^2+q)\, q(q-1)(q-2)(q^2-q)\, I + 4(8_3) \\ &= (n/12)(q-2)(q-4)\, I + 4(8_3).\end{aligned}$$

Putting all the above calculations together we have

$$\begin{aligned}(A_8) &= \tfrac{1}{8}(q^2 - 20q + 120)(A_7) - \tfrac{1}{8}(d_1) \\ &= \tfrac{1}{8}(q^2 - 20q + 120)(A_7) - \tfrac{1}{8}[(q^2 - 14q + 54)(c_1) - 2(d_2) - 2(d_3)] \\ &= \tfrac{1}{8}(q^2 - 20q + 120)[(n/7!)(q-3)(q-5)(q^4 - 20q^3 \\ &\quad + 148q^2 - 468q + 498)\, I - (7_3)] \\ &\quad - \tfrac{1}{8}(q^2 - 14q + 54)[(n/48)(q-3)^2\,(q-4)\, I + 7(7_3)] \\ &\quad + \tfrac{1}{4}[(n/16)(q-3)(q-4)\, I + 21(q-3)(7_3)] \\ &\quad + \tfrac{1}{4}[(n/12)(q-2)(q-4)\, I + 4(8_3)] \\ &= (n/8!)[(q^2 - 20q + 120)(q-3)(q-5) \\ &\quad \times (q^4 - 20q^3 + 148q^2 - 468q + 498) \\ &\quad - 105(q^2 - 14q + 54)(q-3)^2\,(q-4) \\ &\quad + 630(q-3)(q-4) + 840(q-2)(q-4)]\, I + \tfrac{1}{8}[-(q^2 - 20q + 120) \\ &\quad - 7(q^2 - 14q + 54) + 42(q-3)](7_3) + (8_3).\end{aligned}$$

It can be checked that this formula simplifies to that of the theorem.

An idea of the complexity of arcs in finite Desarguesian planes can be gauged from the difficulty of the problem of $(q+2)$-arcs (or "ovals") in $PG(2, q)$, q even. (See [8]. Also see [9] for a generalization to higher-dimensional space.) However, it was shown by B. Segre [16], using a simple algebraic coordinate technique, that every $(q+1)$-arc of $PG(2, q)$

(q odd) is a conic, and so the number of $(q+1)$-arcs in such a projective plane is q^5-q^2.

4.5 THEOREM (Counting configurations in Desarguesian planes). *A finite Desarguesian projective plane is one coordinatized by a finite field $GF(q)$, where q is a prime power. (q is the order of the plane. See, for example,* [11].) *The plane is denoted by $PG(2, q)$.*

Here we give the formulae for the number of variables of size $\leqslant 8$—this gives the reader the possibility of calculating the number of times any configuration with less than 9 points occurs in $PG(2, q)$.

The following hold for $\pi = PG(2, q)$. Note that $n = (q^2+q+1)\times(q+1)\,q^3(q-1)^2$ as before:

$$\text{(i)}\quad (7_3, \pi] = \begin{cases} 0 & \textit{if } q \textit{ is odd,} \\ n/168 & \textit{if } q \textit{ is even.} \end{cases}$$

$$\text{(ii)}\quad (8_3, \pi] = \begin{cases} n/48 & \textit{if}\quad q \equiv 0 \pmod 3, \\ n/24 & \textit{if}\quad q \equiv 1 \pmod 3, \\ 0 & \textit{if}\quad q \equiv 2 \pmod 3). \end{cases}$$

Proof. (i) It is standard theory of $PG(2, q)$ that every 4-arc is contained in a unique subplane of order p, where p is the characteristic of the plane (that is, $q = p^h$, p prime, h a positive integer). When q is odd, it is also well known that $PG(2, q)$ contains no subplane of order 2. (In fact, $PG(2, q)$ contains precisely the subplanes $PG(2, r)$, where $r = p^s$ and s divides h. See [11].) Suppose q is even (that is, $p = 2$ above). The number m of ordered pairs (A_4, f), where A_4 is a model of a 4-arc contained in a model f of a 7_3 contained in π, is

$$m = n/24 = 7(7_3, \pi].$$

This gives the stated value of $(7_3, \pi]$.

(ii) Let the points of $PG(2, q)$ be represented by homogeneous triples (x, y, z) over $GF(q)$. A general 4-arc A_4 may be assumed to have coordinates $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$.

We find the number of configurations 8_3 that contain A_4 and also a general point $(1, \lambda, 0)$ on the line $z = 0$, such that $(0, 0, 1)$ and $(1, 1, 1)$ are not on a line of 8_3. First, one of two possibilities holds: $(1, \lambda, 1) \in 8_3$ or $(0, 1-\lambda, 1) \in 8_3$. These are symmetrical cases, so assume that the former holds. Then it is clear that $(0, 1, 1)$ and $(1, 0, 1-\lambda)$ are also in 8_3. Since $(1, 1, 1)$, $(1, 0, 1-\lambda)$, and $(1, \lambda, 0)$ are collinear, the corresponding 3×3 determinant is zero. This gives

$$\lambda^2 - \lambda + 1 = 0$$

$$\Rightarrow (-\lambda)^3 = 1 \qquad \text{and} \qquad \lambda \neq -1.$$

This last equation has 0, 1, or 2 solutions for $q \equiv 2$, 0 or 1 (mod 3), respectively.

The number of configurations, an A_4 with another point on one of its lines contained in an 8_3, is 24. Hence, by counting these configurations contained in 8_3's contained in π in two ways we obtain

$$24.(8_3, \pi] = (A_4, \pi].\text{ (no. of lines of } A_4).2.(0, 1 \text{ or } 2).$$

Thus,

$$(8_3, \pi] = (n/24).6.2.(0, 1 \text{ or } 2)/24.$$

This is the value stated by the Theorem.

The reader is referred to [1] for a calculation of the number of Pappus 9_3 configurations in $AG(2, q)$, and to [15] for the number of Desargues 10_3 configurations in $PG(2, q)$, for q of characteristic 2 or 3.

4.6 Definition (Blocking sets in projective or affine planes). An *affine plane* is the structure of points and lines obtained by deleting a line and all its points off a projective plane. Its *order* is just the order of the projective plane and so is the number of points on each line. A *blocking set* of a finite projective or affine plane is a set of points that contains no line and is skew to no line. (See for example, [11], for some of the theory of blocking sets.)

4.7 Theorem (Formula for blocking sets). *The number of blocking sets of size k in a projective plane of order q is given by the formula*

$$\sum_{x=0}^{q^2+q+1} \lambda_x \left\{ \binom{q^2+q+1-x}{k-x} + \binom{q^2+q+1-x}{q^2+q+1-k-x} \right\} - \binom{q^2+q+1}{k},$$

where $\lambda_x I = \sum_{c_g = x} (-1)^{|g|} (\bar{g})$ *in* $\Pi(q)$.

Note that c_g is the number of points of a projective plane of order q on the lines of $\bar{g}$—see 3.23. Also, $(\bar{g})$ in $\Pi(q)$ essentially means the number of dual configurations $\bar{g}$ in a plane of order q.

Proof. A blocking set of a projective plane is a set of points which is of type $k.\bar{\Phi}$, such that its complementary set of points is of type $q^2+q+1-k.\bar{\Phi}$. (See 3.23 for the definition of $k.\bar{g}$.) There are three possible types of sets of points of size k of a projective plane:

(a) a blocking set,

(b) a $k.\bar{\Phi}$, whose complement is not a $q^2+q+1-k.\bar{\Phi}$, and

(c) a set of k points containing a line.

Since the number of sets of type (a), (b), and (c) above satisfy in $\Pi(q)$:

$$a+b=(k.\bar{\Phi}),\ a+c=(q^2+q+1-k.\bar{\Phi}),\ a+b+c=\binom{q^2+q+1}{k},$$

$$\text{then } a=(k.\bar{\Phi})+(q^2+q+1-k.\bar{\Phi})-\binom{q^2+q+1}{k}.$$

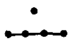
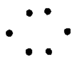
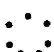
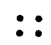
The formula now follows directly from Theorem 3.24b.

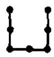
4.8 TABLE (The number of points covered by small dual linear geometries). *Here we list all the* 47 *linear geometries* g *with* $|g| \leqslant 7$, *together with*

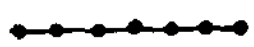
- *the number of points* $|g|$,
- *the size of the group of automorphisms* $[g]$,
- d_g = *the number of flags of* g − *the number of lines of at least* 2 *points of* g, *and*
- $c_g=(q+1)|g|-d_g$ = *the number of points on the lines of* $\bar{g}$, *for* $q=2, 3, 4,$ *and* 5.

Note that "—" denotes that the configuration is not a subgeometry of the projective plane of that order.

i	$g=g_i$	$\|g\|$	$[g]$	d_g	2	3	4	5
1	Φ	0	1	0	0	0	0	0
2	•	1	1	0	3	4	5	6
3	••	2	2	1	5	7	9	11
4		3	6	3	6	9	12	15
5		3	6	2	7	10	13	16
6		4	24	6	6	10	14	18
7		4	6	5	7	11	15	19
8		4	24	3	—	13	17	21
9		5	120	10	—	—	15	20
10		5	12	9	—	11	16	21

i	$g=g_i$	$\lvert g\rvert$	$[g]$	d_g	2	3	4	5
11		5	8	8	7	12	17	22
12		5	24	7	—	13	18	23
13		5	120	4	—	—	21	26
14		6	720	15	—	—	15	21
15		6	36	14	—	—	—	22
16		6	8	13	—	—	17	23
17		6	72	13	—	11	17	23
18		6	6	12	—	12	18	24
19		6	24	11	7	13	19	25
20		6	48	12	—	—	18	24
21		6	12	11	—	13	19	25
22		6	120	9	—	—	21	27
23		6	720	5	—	—	—	31
24		7	7!	21	—	—	—	—
25		7	144	20	—	—	—	—
26		7	16	19	—	—	—	23
27		7	36	19	—	—	—	—

i	$g=g_i$	$\lvert g\rvert$	$[g]$	d_g	2	3	4	5
28		7	8	18	—	—	—	24
29		7	48	18	—	—	17	24
30		7	6	18	—	—	—	—
31		7	6	17	—	—	—	25
32		7	4	17	—	—	18	25
33		7	24	17	—	—	—	25
34		7	12	16	—	12	19	26
35		7	8	16	—	—	—	26
36		7	24	15	—	13	—	27
37		7	168	14	7	—	21	—
38		7	144	18	—	—	—	—
39		7	144	17	—	—	18	25
40		7	12	17	—	—	—	25
41		7	4	16	—	—	19	26

i	$g=g_i$	$\lvert g\rvert$	$[g]$	d_g	2	3	4	5
42		7	6	15	—	13	20	27
43		7	72	15	—	13	20	27
44		7	240	15	—	—	—	27
45		7	48	14	—	—	21	28
46		7	720	11	—	—	—	31
47		7	7!	6	—	—	—	—

4.9 Example (Blocking sets in small projective planes). Here we use the previous table and the formula of Theorem 4.7 to find the number of blocking sets of size k in the projective planes of orders $\leqslant 5$. The percentage in parentheses given after the number of blocking sets b_k below, refers to the percentage of blocking sets of size k out of the total number, $\binom{q^2+q+1}{k}$, of subsets of size k in the plane. This gives a measure of how common these blocking sets are.

Note that all the projective planes of small orders ($q<9$) are self-dual and isomorphic to $PG(2,q)$. Hence $(g)=(\bar{g})$ in $\Pi(q)$, for these small q. Also, as a short-hand notation we usually leave out the I in the constants below. We shall not give all the details of calculating (g_i), as this is quite easy given the small sizes of the configurations. Also, various terms are not necessary because there are no blocking sets of size k for $k<q+\sqrt{q}+1$ (see, for example, [11]), and also $\binom{q^2+q+1-x}{k-x}+\binom{q^2+q+1-x}{q^2+q+1-k-x}$ is zero for all $x>\max(k, q^2+q+1-k)$. Thus it is only necessary know the values of λ_x for $x\leqslant\max(k, q^2+q+1-k)$ in order to calculate the value of b_k.

(i) $q=2$. In this case it can be checked that the number b_k of blocking sets of size k in $PG(2,2)$ is

$$b_k=\left[\binom{7}{k}+\binom{7}{k}\right]-7\left[\binom{4}{k-3}+\binom{4}{k}\right]+21\left[\binom{2}{k-5}+\binom{2}{k}\right]$$
$$-21\left[\binom{1}{k-6}+\binom{1}{k}\right]+6\left[\binom{0}{k-7}+\binom{0}{k}\right]-\binom{7}{k}.$$

It follows then that $b_k=0$, for all $0\leqslant k\leqslant 7$. This is a verification of the well-known fact that there are no blocking sets in $PG(2,2)$.

(ii) $q=3$. We first calculate $\lambda_x I=\sum_{c_g=x}(-1)^{|g|}(g)$ in $\Pi(3)$, for all x from 0 to 11. From the table:

$$\lambda_0=(g_1)=(\Phi)=1.$$
$$\lambda_1=0.$$
$$\lambda_2=0.$$
$$\lambda_3=0.$$
$$\lambda_4=-(g_2)=-13.$$
$$\lambda_5=0.$$
$$\lambda_6=0.$$
$$\lambda_7=(g_3)=13.12/2=78.$$
$$\lambda_8=0.$$
$$\lambda_9=-(g_4)=-13.12.9/3!=-234.$$
$$\lambda_{10}=-(g_5)+(g_6)=-13.4+13.12.9.4/4!=182.$$
$$\lambda_{11}=(g_7)-(g_{10})+(g_{17})=13.4.9-13.4.3.3+13.6=78.$$

The only non-zero value of b_k in fact is for $k=6$ or 7. Then $b_6=b_7=[\binom{13}{6}+\binom{13}{6}]-13[\binom{9}{2}+\binom{9}{6}]+78\binom{6}{6}-\binom{13}{6}=234$ (13.6%).

In fact, one can check that every blocking set of $PG(2,3)$ is a subgeometry g_{19}, which has a complementary g_{36}. Thus, $(g_{19})=(g_{36})=234$ in $\Pi(3)$ (see [11], Theorem 13.4.3).

(iii) $q=4$. We know that a blocking set of size k of $PG(2,4)$ satisfies $7\leqslant k\leqslant 14$, (because $7=4+\sqrt{4}+1$). Hence, to calculate b_k for all k we need to know the values of (g) for $c_g\leqslant 14$. Thus

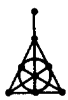
$$\lambda_0=(g_1)=(\Phi)=1.$$
$$\lambda_1=\lambda_2=\lambda_3=\lambda_4=0.$$
$$\lambda_5=-(g_2)=-21.$$
$$\lambda_6=\lambda_7=\lambda_8=0.$$
$$\lambda_9=(g_3)=21.20/2=210.$$
$$\lambda_{10}=\lambda_{11}=0.$$
$$\lambda_{12}=-(g_4)=-21.20.16/3!=-1120.$$
$$\lambda_{13}=-(g_5)=-21.10=-210.$$
$$\lambda_{14}=(g_6)=21.20.16.9/4!=2520.$$

Hence, for $7 \leqslant k \leqslant 14$,

$$b_k = \left[\binom{21}{k} + \binom{21}{k}\right] - 21\left[\binom{16}{k-5} + \binom{16}{k}\right] + 210\left[\binom{12}{k-9} + \binom{12}{k}\right]$$
$$- 1120\left[\binom{9}{k-12} + \binom{9}{k}\right] - 210\left[\binom{8}{k-13} + \binom{8}{k}\right]$$
$$+ 2520\left[\binom{7}{k-14} + \binom{7}{k}\right] - \binom{21}{k}.$$

Thus,

- $b_7 = b_{14} = 360$ (0.3%). Every blocking set of size 7 is a 7_3.
- $b_8 = b_{13} = 15{,}120$ (7.4%). There are two types of blocking sets with 8 points:



(5040),

(10,080).

- $b_9 = b_{12} = 60{,}760$ (20.7%).
- $b_{10} = b_{11} = 109{,}200$ (31.0%).

(iv) $q = 5$. It is known that a blocking set of size k of $PG(2, 5)$ satisfies $9 \leqslant k \leqslant 22$. Hence, to calculate b_k for all k, we need to know the values of (g) for $c_g \leqslant 22$. We shall also calculate the value of the configurations with $c_g = 23$ in order to check that $b_8 = 0$. Thus

$$\lambda_0 = (g_1) = (\Phi) = 1.$$
$$\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 0.$$
$$\lambda_6 = -(g_2) = -31.$$
$$\lambda_7 = \lambda_8 = \lambda_9 = \lambda_{10} = 0.$$
$$\lambda_{11} = (g_3) = 31.30/2 = 465.$$
$$\lambda_{12} = \lambda_{13} = \lambda_{14} = 0.$$
$$\lambda_{15} = -(g_4) = -31.30.25/3! = -3875.$$
$$\lambda_{16} = -(g_5) = -31.6.5.4/3! = -620.$$
$$\lambda_{17} = 0.$$

$$\lambda_{18} = (g_6) = 31.30.25.16/4! = 15{,}500.$$

$$\lambda_{19} = (g_7) = 31.20.25 = 15{,}500.$$

$$\lambda_{20} = -(g_9) = -31.30.25.16.6/5! = -18{,}600.$$

$$\lambda_{21} = (g_8) - (g_{10}) + (g_{14}) = 465 - 93{,}000 + 3100 = -89{,}435.$$

$$\lambda_{22} = -(g_{11}) + (g_{15}) = -46{,}500 + 62{,}000 = 15{,}500.$$

$$\begin{aligned}\lambda_{23} &= -(g_{12}) + (g_{16}) + (g_{17}) - (g_{26}) \\ &= -31.15.25 + 31.15.100 + 31.30.25.16.6.10.3/5!/2 - 3100.15 \\ &= -11{,}625 + 46{,}500 + 279{,}000 - 46{,}500 \\ &= 267{,}375.\end{aligned}$$

Hence, for $8 \leqslant k \leqslant 23$,

$$\begin{aligned} b_k = {} & \left[\binom{31}{k} + \binom{31}{k}\right] - 31\left[\binom{25}{k-6} + \binom{25}{k}\right] + 465\left[\binom{20}{k-11} + \binom{20}{k}\right] \\ & - 3875\left[\binom{16}{k-15} + \binom{16}{k}\right] - 620\left[\binom{15}{k-16} + \binom{15}{k}\right] \\ & + 15{,}500\left[\binom{13}{k-18} + \binom{13}{k}\right] + 15{,}500\left[\binom{12}{k-19} + \binom{12}{k}\right] \\ & - 18{,}600\left[\binom{11}{k-20} + \binom{11}{k}\right] - 89{,}435\left[\binom{10}{k-21} + \binom{10}{k}\right] \\ & + 15{,}500\left[\binom{9}{k-22} + \binom{9}{k}\right] + 267{,}375\left[\binom{8}{k-23} + \binom{8}{k}\right] - \binom{31}{k}. \end{aligned}$$

Thus,

- $b_8 = b_{23} = 0$ (0%).
- $b_9 = b_{22} = 15{,}500$ (.077%).
- $b_{10} = b_{21} = 809{,}100$ (1.8%).
- $b_{11} = b_{20} = 6{,}551{,}850$ (7.7%).
- $b_{12} = b_{19} = 25{,}888{,}875$ (18.3%).
- $b_{13} = b_{18} = 64{,}057{,}625$ (31.1%).
- $b_{14} = b_{17} = 111{,}553{,}500$ (42.1%).
- $b_{15} = b_{16} = 145{,}272{,}200$ (48.3%).

4.10 EXAMPLE (Blocking sets in small affine planes). Here we show how the previous table is used to find the number B_k of blocking sets of size k in all the affine planes of orders $\leqslant 5$. The problem of blocking sets in affine planes is complicated by the fact that two lines may be parallel in such a plane. However, this is compensated by the fact that there are less points to consider than in the corresponding projective plane.

Every affine plane of order $q \leqslant 5$ is isomorphic to $AG(2, q)$, which is obtained from $PG(2, q)$ by deleting a line and all of its points. The method we use is first to calculate the number r_k of sets of size k in the affine plane which intersect each line. That is, the complement of one of these sets in the projective plane is of type $q^2 - k.\bar{g}_2$, where g_2 is the linear geometry with just a single point—see Table 4.8. Then we subtract the number s_k of sets of size k containing at least one line of $AG(2, q)$ and intersecting each line. Thus $B_k = r_k - s_k$. Since every line of $PG(2, q)$ is equivalent to any other line, we may use the following formula for r_k. We are using the fact that $PG(2, q)$ is self-dual and applying Theorem 3.24b. Thus $(g) = (\bar{g})$ in $\Pi(q)$, for these small q.

$$r_k = (q^2+q+1)^{-1}(q^2 - k.\bar{g}_2)$$

$$= (q^2+q+1)^{-1} \sum_{g_j \geqslant g_2, c_j \leqslant q^2+q+1-k} (-1)^{|g_j|-1} |g_j| \binom{q^2+q+1-c_j}{k} (g_j).$$

Hence we first calculate $\zeta_x = (q^2+q+1)^{-1} \sum_{c_g = x+q+1} (-1)^{|g|-1} |g|(g)$ in $\Pi(q)$, for all x from 0 to a large enough size: the size of the largest possible blocking set. We really need to calculate only one of B_k and B_{q^2-k} as they are equal. We then use the formula

$$r_k = \sum_x \zeta_x \binom{q^2 - x}{k}.$$

We shall not give all the details for calculating (g_i), as it is quite easy, given the small sizes of the configurations. s_k will be calculated directly by simple standard methods. Note that it is easier to calculate s_k for smaller values of k, but it is easier to calculate r_k for larger values. Hence we may choose k or $q^2 - k$ as is convenient.

(i) $q = 2$. This case is so small that we note only that there are no blocking sets of $AG(2, 2)$.

(ii) $q = 3$. From Table 4.8:

$\zeta_0 = 13^{-1}(g_2) = 1.$

$\zeta_1 = 0.$

$\zeta_2 = 0.$

$$\zeta_3 = -13^{-1}(g_3).2 = -13^{-1}.13.6.2 = -12.$$
$$\zeta_4 = 0.$$
$$\zeta_5 = 13^{-1}(g_4).3 = 13^{-1}.13.12.9/3!.3 = 54.$$

Hence

$$r_k = \binom{9}{k} - 12\binom{6}{k} + 54\binom{4}{k}, \qquad \text{for} \quad 4 \leqslant k \leqslant 9.$$

Thus $r_9 = 1$, $r_8 = 9$, $r_7 = 36$, $r_6 = 72$, $r_5 = 54$, $r_4 = 0$.

In each case, it is easy to check that $r_k = s_k$. Hence there are no blocking sets in $AG(2, 3)$.

(iii) $q = 4$. From Table 4.8:

$$\zeta_0 = 21^{-1}(g_2) = 1.$$
$$\zeta_1 = 0.$$
$$\zeta_2 = 0.$$
$$\zeta_3 = 0.$$
$$\zeta_4 = -21^{-1}(g_3).2 = -21^{-1}.21.10.2 = -20.$$
$$\zeta_5 = 0.$$
$$\zeta_6 = 0.$$
$$\zeta_7 = 21^{-1}(g_4).3 = 21^{-1}.21.20.16/3!.3 = 160.$$
$$\zeta_8 = 21^{-1}(g_5).3 = 21^{-1}.21.10.3 = 30.$$
$$\zeta_9 = -21^{-1}(g_6).4 = -21^{-1}.21.20.16.9/4!.4 = -480.$$
$$\zeta_{10} = 21^{-1}[-(g_7).4 + (g_9).5 - (g_{14}).6] = -640 + 240 - 48 = -448.$$

Hence

$$r_k = \binom{16}{k} - 20\binom{12}{k} + 160\binom{9}{k} + 30\binom{8}{k} - 480\binom{7}{k} - 448\binom{6}{k}, \qquad \text{for} \quad 6 \leqslant k \leqslant 16.$$

Thus $r_{16} = 1$, $r_{15} = 16$, $r_8 = 4440$, $r_7 = 1120$, $r_6 = 0$.

Since $r_6 \geqslant s_6$, then $s_6 = 0$ and $B_6 = r_6 - s_6 = 0$. We do not have to consider any $k \leqslant 5$ because from Table 4.8, $|g| \leqslant 5$ and $c_g \geqslant 20 \Rightarrow g = g_{13}$. This line of 5 points certainly does not correspond to a blocking set of $AG(2, 4)$.

Consider the sets of 7 points of $AG(2, 4)$ which contain a line and intersect every line. There are then two possibilities, containing either 1 or 2 lines: let a be the number of sets of type $3.\bar{g}_2$, and let b be the number of sets of type $0.\bar{g}_3$. We then have $b = 16.10 = 160$, and $a + 2b = 20.4^3 = 1280$. Hence $s_7 = a + b = 1120$. Thus $B_7 = r_7 - s_7 = 0$.

Consider the sets of 8 points of $AG(2, 4)$ that contain a line and intersect every line. There are then two possibilities, containing either 1 or 2 lines: let a be the number of sets of type $4.\bar{g}_2$, and let b be the number of sets of type $1.\bar{g}_3$. We now have $b = 16.10.9 = 1440$, and $a + 2b = 20.3.6.4.4 = 5760$. Hence $s_8 = a + b = 5760 - 1440 = 4320$. Thus $B_8 = r_8 - s_8 = 4440 - 4320 = 120$. It is quite easy to check that each of these blocking sets is a configuration 8_3, which must therefore have a complementary configuration of the same type.

There is no need to consider the sets of size 9 because they are complementary to subsets of size 7. Hence we have just shown that there are exactly 120 blocking sets of $AG(2, 4)$, and these all give an 8_3 subgeometry.

(iv) $q = 5$. From Table 4.8:

$\zeta_0 = 31^{-1}(g_2) = 1.$

$\zeta_1 = 0.$

$\zeta_2 = 0.$

$\zeta_3 = 0.$

$\zeta_4 = 0.$

$\zeta_5 = -31^{-1}(g_3).2 = -31^{-1}.31.15.2 = -30.$

$\zeta_6 = 0.$

$\zeta_7 = 0.$

$\zeta_8 = 0.$

$\zeta_9 = 31^{-1}(g_4).3 = 31^{-1}.31.30.25/3!.3 = 375.$

$\zeta_{10} = 31^{-1}(g_5).3 = 31^{-1}.31.20.3 = 60.$

$\zeta_{11} = 0.$

$\zeta_{12} = -31^{-1}(g_6).4 = -31^{-1}.31.30.25.16/4!.4 = -2000.$

$\zeta_{13} = -31^{-1}(g_7).4 = -31^{-1}.31.20.25.4 = -2000.$

$\zeta_{14} = 31^{-1}(g_9).5 = 31^{-1}.31.30.25.16.6/5!.5 = 3000.$

$\zeta_{15} = 31^{-1}[-(g_8).4 + (g_{10}).5 - (g_{14}).6] = -60 + 15{,}000 - 600 = 14{,}340.$

$\zeta_{16} = 31^{-1}[(g_{11}).5 - (g_{15}).6] = 7500 - 12{,}000 = -4500.$

$\zeta_{17} = 31^{-1}[-(g_{12}).5 + (g_{16}).6 - (g_{17}).6 + (g_{26}).7]$
$= 1875 - 54{,}000 - 9000 + 10{,}500 = -50{,}625.$

Hence for $8 \leqslant k \leqslant 25$,

$$r_k = \binom{25}{k} - 30\binom{20}{k} + 375\binom{16}{k} + 60\binom{15}{k} - 2000\binom{13}{k} - 2000\binom{12}{k} + 3000\binom{11}{k} + 14{,}340\binom{10}{k} - 4500\binom{9}{k} - 50{,}625\binom{8}{k}.$$

Thus,

$$\begin{aligned}
r_{25} &= 1,\\
r_{24} &= 25,\\
r_{23} &= 300,\\
r_{22} &= 2300,\\
r_{21} &= 12{,}650,\\
r_{20} &= 53{,}100,\\
r_{19} &= 176{,}500,\\
r_{18} &= 475{,}000,\\
r_{17} &= 1{,}047{,}375,\\
r_{16} &= 1{,}898{,}000,\\
r_{15} &= 2{,}809{,}700,\\
r_{14} &= 3{,}340{,}500,\\
r_{13} &= 3{,}089{,}000,\\
r_{12} &= 2{,}103{,}000,\\
r_{11} &= 961{,}500,\\
r_{10} &= 252{,}600,\\
r_{9} &= 28{,}375.\\
r_{8} &= 0.
\end{aligned}$$

We do not have to consider any $k \leqslant 7$ because, from Table 4.8, there is no linear geometry g with $|g| \leqslant 7$ and $c_g = 30$.

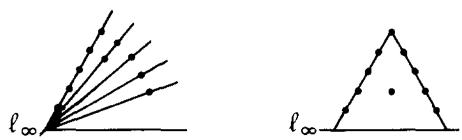
Since $r_8 = 0$ we have $B_8 = 0$.

Consider the sets of 9 points of $AG(2,5)$ that contain a line and intersect every line. There are then two possibilities, containing either 1 or 2 lines:

let a be the number of sets of type $4.\bar{g}_2$, and let b be the number of sets of type $0.\bar{g}_3$ (see the following diagram).

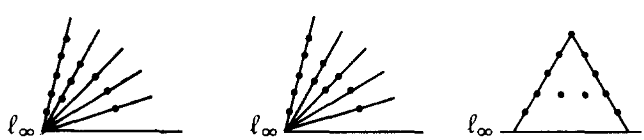
We have $b = 25.15 = 375$, and $a + 2b = 30.5^4$. Hence $s_9 = a + b = 5^3(150 - 3) = 125.147 = 18{,}375$. Thus $B_9 = r_9 - s_9 = 28{,}375 - 18{,}375 = 10{,}000$. (This is 0.49 % of the total number of subsets of size 9 of $AG(2,5)$.)

Consider the sets of 10 points of $AG(2,5)$ that contain a line and intersect every line. There are then two possibilities, containing either 1 or 2 lines: let a be the number of sets of type $5.\bar{g}_2$, and let b be the number of sets of type $1.\bar{g}_3$ (see the following diagram).



We have that $b = 25.15.16 = 6000$, and $a + 2b = 30.4.10.5^3 = 150{,}000$. Hence $s_{10} = a + b = 150{,}000 - 6000 = 144{,}000$. Thus $B_{10} = r_{10} - s_{10} = 252{,}600 - 144{,}000 = 108{,}600$. (This is 3.32% of the total number of subsets of size 10 of $AG(2, 5)$.)

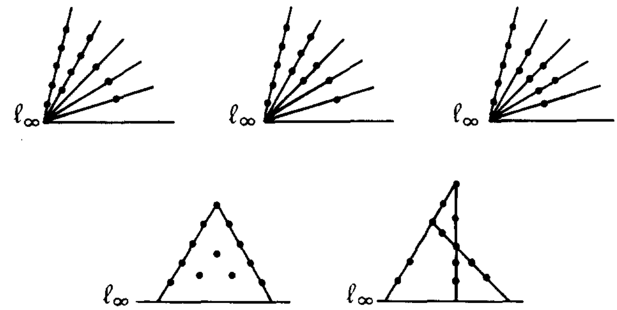
Consider the sets of 11 points of $AG(2,5)$ that contain a line and intersect every line. There are then three possibilities, containing either 1 or 2 lines: let a be the number of sets of type $6.\bar{g}_2$, and let b be the number of sets of type $2.\bar{g}_3$ (see the following diagram).



We have $b = 25.15.16.15/2 = 45{,}000$, and $a + 2b = 30.4.10.5^3 + 30.6.10^2.5^2 = 600{,}000$. Hence $s_{11} = a + b = 600{,}000 - 45{,}000 = 555{,}000$. Thus $B_{11} = r_{11} - s_{11} = 961{,}500 - 555{,}000 = 406{,}500$. (This is 9.12% of the total number of subsets of size 11 of $AG(2,5)$.)

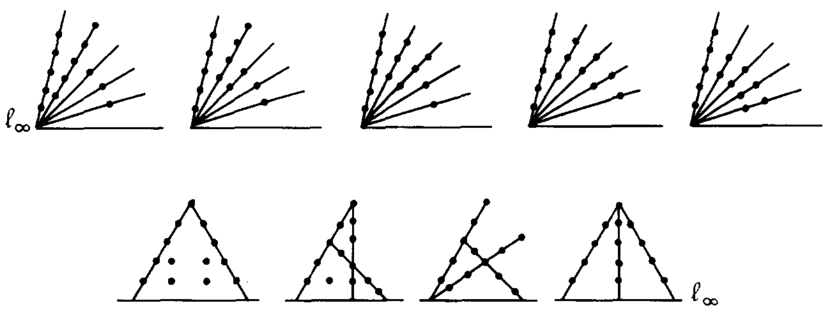
Consider the sets of 12 points of $AG(2,5)$ that contain a line and intersect every line. There are then five possibilities, containing 1, 2, or 3 lines: let a

be the number of sets of type $7.\bar{g}_2$, let b be the number of sets of type $3.\bar{g}_3$, and let c be the number of sets of type $0.\bar{g}_4$ (see the following diagram).



We have $c = 20.5.5.4 = 2000$, and $b + 3c = 25.15.16.15.14/3! = 210{,}000$, and $a + 2b + 3c = 30(4.5.5^3 + 4.10.3.10.5.5 + 4.10^3.5) = 30(2500 + 30{,}000 + 20{,}000) = 1{,}575{,}000$. Hence $s_{12} = a + b + c = 1{,}575{,}000 - 210{,}000 + 2000 = 1{,}367{,}000$. Thus $B_{12} = r_{12} - s_{12} = 2{,}103{,}000 - 1{,}367{,}000 = 736{,}000$. (This is 14.16% of the total number of subsets of size 12 of $AG(2,5)$.)

Consider the sets of 13 points of $AG(2,5)$ that contain a line and intersect every line. There are then nine possibilities, containing 1, 2, or 3 lines: let a be the number of sets containing 1 line, let b be the number of sets containing 2 lines, and let c be the number containing 3 lines (see the following diagram).



We have $c = 2000.13 + 25.20 + 6.10.25 = 26{,}000 + 500 + 1500 = 28{,}000$. Also $b + 3c = 6.10.5^3 + 25.15.16.15.14.13/4! = 7500 + 682{,}500 = 690{,}000$. And $a + 2b + 3c = 30(4.5^3 + 4.3.5.10.5.5 + 6.10^2.5^2 + 4.3.10^3.5 + 10^4) = 30(500 + 15{,}000 + 15{,}000 + 60{,}000 + 10{,}000) = 3{,}015{,}000$. Hence $s_{13} = a + b + c = 3{,}015{,}000 - 690{,}000 + 28{,}000 = 2{,}353{,}000$. Thus $B_{13} = r_{13} - s_{13} = 3{,}089{,}000 - 2{,}353{,}000 = 736{,}000$. (This checks with the value of B_{12} attained above.)

Summarizing, we have found the number B_k of blocking sets of $AG(2,5)$ to be

$$\begin{aligned} B_0 &= B_1 = \cdots = B_8 = 0, \\ B_9 &= B_{16} = 10{,}000 \ (0.49\%), \\ B_{10} &= B_{15} = 108{,}600 \ (3.32\%), \\ B_{11} &= B_{14} = 406{,}500 \ (9.12\%), \\ B_{12} &= B_{13} = 736{,}000 \ (14.16\%). \end{aligned}$$

4.11 Example (Blocking sets in $\pi(10)$). Suppose we wish to calculate the number b_{55} of blocking sets of size 55 in a projective plane of order 10. Using the formula of Theorem 4.7, we have

$$b_{55} = \sum_{x=0}^{111} \lambda_x \left\{ \binom{111-x}{55-x} + \binom{111-x}{56-x} \right\} - \binom{111}{55},$$

where $\lambda_x I = \sum_{c_g = x} (-1)^{|g|} (\bar{g})$ in $\Pi(10)$.

Since the coefficient with λ_x above is zero when $x > 56$, we need to calculate only the value of λ_x for $0 \leqslant x \leqslant 56$. That is, we need only to know the number of configurations in a plane of order 10 having $c_g \leqslant 56$. We have shown how to calculate the formula for any configuration with $\leqslant 6$ points—it is a constant. For the configurations g with $\geqslant 7$ points it is easy to show that c_g is $\leqslant 56$ if and only if g is a 7-arc A_7 of the plane. (The k-arcs in general have the least "covering" numbers.) From Theorem 3.16, λ_x is an easily calculated constant for $x < 56$ and for $x = 56$ it is equal to a constant $-(A_7)$ in $\Pi(10)$. From Theorem 4.2, it follows that λ_{56} is equal to a constant + the number (7_3) of Fano subplanes of the plane. (Note that these calculations are actually for the dual plane, but this does not matter since the 7_3 is self-dual. In fact, since 8_3 is also self-dual, the number of linear subgeometries of a certain type with $\leqslant 8$ points in any finite projective plane is equal to the number in its dual.)

From the above formula it follows that b_{55} is equal to a constant $K+$ the number (7_3) of subplanes of order 2 in the plane of order 10. We leave it to the interested reader to calculate the constant K.

4.12 Theorem (An indirect construction of blocking sets). *Here we present an indirect construction of blocking sets in finite projective planes. Let M be a set of $q+1$ lines of a projective plane π of order q. Let S be the set of points of π on at least 2 lines of M. Then S is "usually" a blocking set. (This result is in the spirit of "asymptotic" geometry as expounded in the introduction to the paper by B. Segre [17].)*

Proof. First it is clear that S contains no complete line—each line in M contains at most q points of S, and each line not in M contains at most $\frac{1}{2}(q+1)$ points of S. There remains to show that every line of π contains at least one point of S—that is, no line intersects the $q+1$ lines of M such that each of its $q+1$ points is on a unique line of M. The number of the latter diagrams in π is $d=(q^2+q+1)\,q^{q+1}$. If we can show that d is less than the number e of sets of lines of size $q+1$ in π, it follows that there are sets of lines giving blocking sets. In particular, if we can show that $d \ll e$, for q large enough, then it follows that "most" sets of $q+1$ lines of a projective plane of order q give a blocking set.

We must show that $d=(q^2+q+1)\,q^{q+1} \ll e = \binom{q^2+q+1}{q+1}$, for q large enough. Now

$$e=((q^2+q+1)/(q+1))\cdot((q^2+q)/q)\cdots((q^2+3)/3)\cdot((q^2+2)/2)\cdot(q^2+1).$$

Thus $e>q^{q-2}\cdot(q^2/3)\cdot(q^2/2)\cdot q^2 \Rightarrow e>q^{q+4}/6$.
Hence $d/e<6\cdot(q^2+q+1)/q^3$.

This holds if $q \geqslant 7$; in fact the ratio $d/e \to 0$ as $q \to \infty$. We can also check that if $q=5$ or 6 then $d<e$.

Conclusions

In "Rings of Geometries I," the reader was shown a way of creating well-defined "geometrical structures" on different kinds of combinatorial objects. The reason was to create a kind of "black box" that could be used to solve various kinds of combinatorial problems involving substructures of these objects. This paper shows how to use the black box to solve problems in finite plane theory. However, as with any new technique, ad hoc methods still have to be used to achieve results with sufficient simplicity.

The main emphasis of the paper is to count configurations in finite projective planes, but behind this superficiality is the hope that a better understanding of these methods will lead to powerful proofs for the existence or non-existence of various kinds of geometrical structures. One way to show the non-existence would be to find collections of subgeometries and positive coefficients for each of them such that the number of times they occur in the putative geometry is negative. The example given in this paper is that the projective plane of order 6 does not exist because the sum of the 7-arcs plus the Fano subplanes is negative in the ring of such a plane. A problem with this approach is the following. The investigation of larger planes (for example, of order 10) must deal with larger configurations. It is proposed to deal with this problem by considering more expansive definitions of subgeometry. This is why the general theory of "Rings of Geometries I" is useful—it is possible to vary the definition of subgeometry to suit the precise problem, but also to remain within the same general framework. This allows the development of formulae that relate the numbers involving the different definitions and allows us to produce results unattainable by other means.

The example in this paper of counting blocking sets is of significance. The logic of the author in attacking this problem was as follows. First, the methods to date were either to construct blocking sets directly using well-known configurations or to calculate them directly in the small planes. Second, since the number of configurations increases exponentially with size, the "direct" methods soon run into difficulty. The main idea was to use a definition of subgeometries in projective planes that "brought out" the numbers involved with blocking sets. Since complete lines are important for blocking sets, the type of geometry to define was obviously the "complete-line geometry" (see Definition 3.23). This led directly to the formulae (3.24) that convert them to the standard linear geometries. Then it was straightforward to derive the formula for blocking sets, which is obviously a much more efficient way to calculate the numbers of larger-sized blocking sets than the direct method. Once the number of blocking sets of a certain size is known, it makes the direct classification of the actual blocking sets much easier.

Finally, it is observed that the connection between a projective plane and its dual has still not been fully exploited. Perhaps there are deeper formulae relating the plane and its dual and perhaps these will lead to improvements on the "fundamental theorems" of 3.16 and 3.21. (Obviously Theorem 3.21 deals with both points and lines simultaneously, but we have still not *used* this connection to obtain some substantial results. Also, the formulae of 3.24 relate the plane and its dual.) It is clear that there are many more basic results to be found. Also of interest would be an extension of these methods to types of combinatorial structures other than finite projective and affine planes.

References

1. E. Bohne and R. Möller, Über die Anzahl projektiver PAPPOS-Konfigurationen in endlichen desarguesschen affinen Inzidenzebenen, *Beiträge Algebra Geom.* **17** (1984), 23–30.
2. R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. J. Math.* **1** (1949), 88–93.
3. J. van der Craats, On Simonis' 10_3 configuration, *Nieuw Arch. Wisk.* (4) **1** (1983), 193–207.
4. P. Dembowski, "Finite Geometries," Springer, New York, 1968.
5. J. Doyen, "Sur les espaces linéaires finis," Mémoire de licence, pp. 60–82, University of Brussels, 1967.

6. J. DOYEN, Sur le nombre d'espaces linéaires non isomorphes de n points, *Bull. Soc. Math. Belg.* **19** (1967), 421–437.
7. P. ERDŐS, R. C. MULLIN, V. T. SOS, AND D. R. STINSON, Finite linear spaces and projective planes, *Discrete Math.* **47** (1983), 49–62.
8. D. G. GLYNN, Two new sequences of ovals in finite Desarguesian planes of even order, *in* "Combinatorial Math. X," (Adelaide 1982), pp. 217–229; Lecture Notes in Math., Vol. 1036, Springer, Berlin/Heidelberg/New York/Tokyo, 1983.
9. D. G. GLYNN, The non-classical 10-arc of $PG(4,9)$, *Discrete Math.* **59** (1986), 43–51.
10. D. G. GLYNN, Rings of geometries I, *J. Combin. Theory Ser. A* **44** (1987), 34–48.
11. J. W. P. HIRSCHFELD, "Projective Geometries over Finite Fields," Oxford Univ. Press, Oxford, 1979.
12. D. R. HUGHES AND F. C. PIPER, "Projective Planes," Springer, New York/Heidelberg/Berlin, 1973.
13. S. KANTOR, Die Konfigurationen $(3,3)_{10}$, *Sitzungsber. Akad. Wiss. Wien, Math.-Natur. Kl.* **84** (1881), 1291-1314.
14. C. W. H. LAM, L. THIEL, S. SWIERCZ, AND J. MCKAY, The nonexistence of ovals in a projective plane of order 10, *Discrete Math.* **45** (1983), 319–321.
15. R. PUYSTJENS AND J. A. THAS, The number of Desargues-configurations of the projective plane $S_{2,q}$ over the Galois field $GF(q)$ with characteristic two or three, *Simon Stevin* **44** (1971), 160–170.
16. B. SEGRE, Sulle ovali nei piani lineari finiti, Atti Accad. Naz. Lincei Rend. *Cl. Sci. Fis. Mat. Natur.* (8) **17** (1954), 1–2.
17. B. SEGRE, Le geometrie di Galois, *Ann. Mat. Pura Appl.* (4) **48** (1959), 1–95.
18. N. J. A. SLOANE, "A Handbook of Integer Sequences," Academic Press, New York/London, 1973.