A coding theoretic approach to the uniqueness conjecture for projective planes of prime order

Bhaskar Bagchi

Abstract

An outstanding folklore conjecture asserts that, for any prime \( p \), up to isomorphism the projective plane \( PG(2, \mathbb{F}_p) \) over the field \( \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} \) is the unique projective plane of order \( p \). Let \( \pi \) be any projective plane of order \( p \). For any partial linear space \( \mathcal{X} \), define the inclusion number \( i(\mathcal{X}, \pi) \) to be the number of isomorphic copies of \( \mathcal{X} \) in \( \pi \). In this paper we prove that if \( \mathcal{X} \) has at most \( \log_2 p \) lines, then \( i(\mathcal{X}, \pi) \) can be written as an explicit rational linear combination (depending only on \( \mathcal{X} \) and \( p \)) of the coefficients of the complete weight enumerator (c.w.e.) of the \( p \)-ary code of \( \pi \). Thus, the c.w.e. of this code carries an enormous amount of structural information about \( \pi \). In consequence, it is shown that if \( p > 2^9 = 512 \), and \( \pi \) has the same c.w.e. as \( PG(2, \mathbb{F}_p) \), then \( \pi \) must be isomorphic to \( PG(2, \mathbb{F}_p) \). Thus, the uniqueness conjecture can be approached via a thorough study of the possible c.w.e. of the codes of putative projective planes of prime order.

Keywords Projective planes · Complete weight enumerator · Partial linear spaces · Inclusion numbers · Pappus’ Configuration

Mathematics Subject Classification Primary 05B25 · Secondary 68P30

1 Introduction

An incidence system is a pair \( (P, L) \) where \( P \) is a set, and \( L \) is a set of subsets of \( P \). The elements of \( P \) and \( L \) are called the points and lines (or blocks) of the incidence system. If \( x \) is a point and \( \ell \) is a line, then we say that \( x \) and \( \ell \) are incident with each other if \( x \in \ell \).

For any two incidence systems \( \mathcal{X} = (P, L) \) and \( \mathcal{X}' = (P', L') \), we say that \( \mathcal{X}' \) is a subsystem of \( \mathcal{X} \) if \( P' \subseteq P \), and every \( \ell' \in L' \) can be written as \( \ell' = \ell \cap P' \) for some \( \ell \in L \).

Let \( \mathcal{X} = (P, L) \) and \( \mathcal{X}' = (P', L') \) be two incidence systems. If \( f : P \rightarrow P' \) and \( g : L \rightarrow L' \) are functions such that, for all \( x \in P \) and \( \ell \in L \), \( x \in \ell \Rightarrow f(x) \in g(\ell) \), then we say that the pair \( (f, g) \) is a homomorphism from \( \mathcal{X} \) to \( \mathcal{X}' \). If, further, both \( f \) and

Communicated by L. Storme.
are one-to-one, then we say that \((f, g)\) is a monomorphism from \(X\) to \(X'\). If both \(f\) and \(g\) are onto then \((f, g)\) is called an epimorphism from \(X\) to \(X'\), and we say that \(X'\) is a homomorphic image of \(X\). An isomorphism from \(X\) to \(X'\) is a homomorphism which is both a monomorphism and an epimorphism. If there is an isomorphism from \(X\) to \(X'\), then we say that \(X\) and \(X'\) are isomorphic. One often identifies isomorphic incidence systems. Note that any monomorphism from \(X\) to \(X'\) may be viewed as an isomorphism between \(X\) and a subsystem of \(X'\). An automorphism of \(X\) is an isomorphism from \(X\) to \(X\). The set \(\text{Aut}(X)\) of all automorphisms of \(X\) forms a group (the automorphism group of \(X\)) under componentwise composition.

An incidence system \(X\) is said to be a partial linear space if (a) each line of \(X\) is incident with at least two points, and (b) any two distinct points of \(X\) are together incident with at most one line of \(X\). We say that \(X\) is a linear space if it satisfies (a) and (b'): any two distinct points of \(X\) are together incident with a unique line of \(X\). Note that if \((f, g)\) is a monomorphism from a partial linear space \(X\) to a partial linear space \(X'\), then \(g\) is determined by \(f\) in view of the requirement \(f(\ell) \subseteq g(\ell) (\ell \in L)\). (Here \(f(\ell) := \{f(x) : x \in \ell\}\).) In this case, it is usual to omit mention of \(g\), and one says that \(f\) is the monomorphism. In particular, this remark applies to isomorphisms and automorphisms of partial linear spaces.

If \(X\) is a partial linear space, then its dual \(X^*\) is the incidence system obtained from \(X\) by interchanging the notions of points and lines. More precisely, the incidence system \(X^* = (P^*, L^*)\) is the dual of \(X = (P, L)\) if there are bijections \(f : P \rightarrow L^*, g : L \rightarrow P^*\) such that, for all \(x \in P\) and \(\ell \in L\), \(x \in \ell \iff g(\ell) \in f(x)\). This defines the dual up to isomorphisms. Note that the dual \(X^*\) of a partial linear space \(X\) is again a partial linear space iff each point of \(X\) is incident with at least two lines of \(X\). In this case, we have \(X^{**} = X\).

Finally, a projective plane is an incidence system \(X\) such that (i) \(X\) is a linear space, (ii) its dual \(X^*\) is also a linear space, and (iii) given any two distinct lines of \(X\), there is at least one point of \(X\) which is non-incident with both lines. Note that, in the presence of (i) and (ii), the condition (iii) is equivalent to its dual condition (iii)*: given any two distinct points of \(X\), there is at least one line of \(X\) which is non-incident with both points. Thus, the dual of a projective plane is a projective plane (see \([5\text{, pp. 115–116}]\), \([9\text{, pp. 77–78}]\)).

If \(x_1, x_2\) are distinct points of a projective plane, we shall denote by \(x_1 \vee x_2\) the unique line incident with both \(x_1\) and \(x_2\). Dually, if \(\ell_1, \ell_2\) are distinct lines of a projective plane, then \(\ell_1 \wedge \ell_2\) denotes the unique point incident with both \(\ell_1\) and \(\ell_2\). Note that, for any non-incident point line pair \((x, \ell)\), \(y \mapsto x \vee y\) defines a function from the set of all points on \(\ell\) to the set of all lines through \(x\). Clearly the function \(m \mapsto m \wedge \ell\) from the set of all lines through \(x\) to the set of all points on \(\ell\) is its inverse. So these two functions are bijections. These bijections are the so-called perspectivities between the lines through \(x\) and the points on \(\ell\) in the projective plane (see \([5\text{, pp. 157–158}]\)). The existence of these perspectivities may be used to see that if \(\pi\) is a finite projective plane, then there is a number \(n \geq 2\) such that (a) each point of \(\pi\) is incident with exactly \(n + 1\) lines, (b) each line of \(\pi\) is incident with exactly \(n + 1\) points, (c) the total number of points of \(\pi\) is \(n^2 + n + 1\), and (d) the total number of lines of \(\pi\) is \(n^2 + n + 1\). This number \(n\) is called the order of the finite projective plane \(\pi\) (see \([9\text{, p. 79}]\)).

Examples (1) The field planes Let \(V\) be a three dimensional vector space over a field \(F\). For \(i = 1, 2\), let \(V_i\) be the set of all \(i\)-dimensional vector subspaces of \(V\). We identify each element \(\ell\) of \(V_2\) with the set of all elements of \(V_1\) contained in \(\ell\). With this identification, \(PG(2, F) := (V_1, V_2)\) is a projective plane, called the projective plane over \(F\). (This is the two-dimensional case of the more general construction described in \([5\text{, p. 158}\]\) and \([9\text{, pp. 24–25}\]\).) With a little care in handling non-commutativity of multiplication, this construction generalizes to yield the projective plane \(PG(2, D)\) over any division ring \(D\). Recall that, by a famous theorem of Wedderburn, the finite fields \(F_q\) (\(q\) prime power) are the only finite
division rings. Specializing the above construction, we get the classical finite projective planes $PG(2, \mathbb{F}_q)$, of order $q$.

(2) The free projective plane The usual definition of the free projective plane may be found in [9, Chap. 11]. We like to rephrase this definition slightly, as follows. We first define a sequence $\mathcal{X}_n = (P_n, L_n), n \geq 1$, of partial linear spaces by induction on $n$. $\mathcal{X}_1$ is the incidence system whose points and lines are the vertices and edges of the 4-cycle. That is, $\mathcal{X}_1 = (P_1, L_1)$, where $P_1 = \{1, 2, 3, 4\}$ and $L_1 = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Having defined $\mathcal{X}_n$, we extend it to $\mathcal{X}_{n+1}$ by introducing a new point $\ell_1 \land \ell_2$ corresponding to each pair $\{\ell_1, \ell_2\}$ of lines of $\mathcal{X}_n$ such that no point of $\mathcal{X}_n$ is incident in $\mathcal{X}_n$ with both $\ell_1$ and $\ell_2$, and introducing a new line $x_1 \lor x_2$ corresponding to each pair $\{x_1, x_2\}$ of points of $\mathcal{X}_n$ such that no line of $\mathcal{X}_n$ is incident in $\mathcal{X}_n$ with both $x_1$ and $x_2$. The point $\ell_1 \land \ell_2$ is incident in $\mathcal{X}_{n+1}$ with the lines $\ell_1, \ell_2$ and with no other line. The line $x_1 \lor x_2$ is incident in $\mathcal{X}_{n+1}$ with the points $x_1, x_2$ and with no other point. The incidences between the old points and old lines are as in $\mathcal{X}_n$. Thus, by construction, each $\mathcal{X}_n$ is a subsystem of $\mathcal{X}_{n+1}$. Finally, we define $\mathcal{F} = \left(\bigcup_{n=1}^{\infty} P_n, \bigcup_{n=1}^{\infty} L_n\right)$. Clearly $\mathcal{F}$ is an (infinite) projective plane. It is called the free projective plane. An easy induction shows that each $\mathcal{X}_n$ is self-dual (i.e., isomorphic to its dual). It follows that (like the field planes) the free projective plane is self dual.

A projective plane $\sigma$ is said to be a subplane of the projective plane $\pi$ if $\sigma$ is a subsystem of $\pi$. A projective plane $\pi$ is said to be prime if it has no proper projective subplane. The projective planes over prime fields $\mathbb{F}$ (i.e., $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F} = \mathbb{F}_p$ for some prime $p$) are obvious examples of prime projective planes. It is not hard to see that the free projective plane $\mathcal{F}$ is also prime. Indeed, using the above construction, one sees that the automorphism group of $\mathcal{F}$ is transitive on the 4-cycles - isomorphic copies of $\mathcal{X}_1$ - in $\mathcal{F}$. By elementary linear algebra, the same is true of $PG(2, \mathbb{F})$, $\mathbb{F}$ a field. Now let $\pi$ be a projective plane over a prime field, or $\pi = \mathcal{F}$. Since any sub-plane of $\pi$ would contain a 4-cycle, and the group of $\pi$ is transitive on 4-cycles, in order to prove that $\pi$ is a prime plane, it suffices to show that some suitable 4-cycle $C$ in $\pi$ generates $\pi$. Choose $C = \mathcal{X}_1$ if $\pi = \mathcal{F}$, and choose $C$ to be any 4-cycle with point set $\{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1)\}$ if $\pi$ is a projective plane over a prime field. Then, by construction in case $\pi = \mathcal{F}$ and by an elementary computation in case $\pi = PG(2, \mathbb{F})$, $\mathbb{F}$ a prime field, one sees that such a cycle $C$ generates $\pi$. Therefore $\pi$ is a prime projective plane. In a private conversation with the author some years back, N.M. Singhi forwarded:

**Conjecture 1.1** (Singhi) The projective planes over prime fields and the free projective plane are the only examples of prime projective planes.

One of the reasons why the free projective plane is important is the fact that every prime projective plane is a homomorphic image of $\mathcal{F}$. (Indeed, given a prime projective plane $\pi$, one may readily find a monomorphism $f_1$ of $\mathcal{X}_1$ into $\pi$. Hence one may inductively construct a homomorphism $f_n$ of $\mathcal{X}_n$ into $\pi$ such that $f_{n+1}$ extends $f_n$ for each $n$. Then $f := \bigcup_{n=1}^{\infty} f_n$ is a homomorphism from $\mathcal{F}$ into $\pi$. Since $\pi$ is prime, $f$ must be an epimorphism.) This indicates that an in-depth study of the partial linear spaces $\mathcal{X}_n$ may be an useful approach to Singh’s conjecture. Note that, in particular, if $\pi$ is a finite prime projective plane, then it follows from the above that $\pi$ is a homomorphic image of $\mathcal{X}_n$ for sufficiently large $n$. We suggest that an investigation of the codes of $\mathcal{X}_n$ (over various primes) may be fruitful. But we do not even know a formula for the number $v_n$ of points (= number of lines) of $\mathcal{X}_n$. The sequence $\{v_n\}$ begins with $4, 6, 7, 9, 13, 33, \ldots$.

When $q$ is a “genuine” prime power (i.e., $q = p^f$, $p$ prime, $e \geq 2$) and $q > 8$, there are many constructions of projective planes of order $q$ which are not field planes. But no such construction is known for $q = p$. The subject of this paper is the following
Conjecture 1.2 (folklore) Up to isomorphism, $PG(2, \mathbb{F}_p)$ is the only projective plane of prime order $p$.

Conjecture 1.2 bears a superficial resemblance to Singhi’s conjecture. But the relationship between these two is far from clear. We do not even know if a projective plane of prime order must be a prime projective plane, or if a prime projective plane which is finite must be of prime order. Another related conjecture is due to Neumann [11] (which is much stronger than the finite case of Singh’s conjecture):

Conjecture 1.3 (Neumann) A finite projective plane has no projective subspace of order two (if and) only if it is isomorphic to $PG(2, \mathbb{F}_q)$ for some odd prime power $q$.

In the humble opinion of this author, the uniqueness Conjecture 1.2 is one of the most beautiful and important open problems in mathematics. It is amusing as well as sad that it finds no mention in the lists of “problems for the new millenium” compiled by various authors at the turn of the century. It is not lacking in history and pedigree. With some imagination, one may trace the history of such problems in finite geometry back to Euler’s 1782 paper [6] on the problem of the thirty six officers. The projective planes $PG(2, \mathbb{F}_p)$ were first constructed by von Staudt [14] in 1856. They were generalized to the planes $PG(2, \mathbb{F}_q)$, $q$ prime power, by Fano [8] in 1892. The first examples of non-field finite projective planes were constructed by Veblen and Wedderburn [13] in 1907. Conjecture 1.2 must have occurred to these early authors. The vast literature on finite projective planes includes (usually as special cases) many characterizations of $PG(2, \mathbb{F}_p)$ on the assumption of moderately large automorphism groups. See [9] and [5, Chap. 5] for many of these results.

2 Coding theory

One very fruitful approach to problems in finite geometry has been through the study of codes attached to these geometries. For a comprehensive account of these connections, the reader may consult [1].

If $P$ is a finite set and $p$ is a prime number, then consider the $\mathbb{F}_p$-vector space $\mathbb{F}_p^P$ consisting of all functions $f : P \to \mathbb{F}_p$. For any such $f$, the support of $f$ is the set $\{x \in P : f(x) \neq 0\}$, and the Hamming weight $|f|$ of $f$ is the size (cardinality) of the support of $f$. The type of $f$, denoted by $\text{type}(f)$, is the $p$-tuple $(\alpha_0 : \alpha \in \mathbb{F}_p)$ where $\alpha_0 = \# \{x \in P : f(x) = \alpha\}$. $\mathbb{F}_p^P$ is a metric space with the Hamming metric given by $d(f, g) = |f - g|$. One also equips $\mathbb{F}_p^P$ with the usual non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ defined by $\langle f, g \rangle = \sum_{x \in P} f(x)g(x)$.

A $p$-ary code $C$ is a linear subspace of $\mathbb{F}_p^P$, viewed as a metric space with the Hamming metric inherited from $\mathbb{F}_p^P$. The vectors in $P$ are called the words of $C$. The elements of $P$ are called the coordinates positions of $C$. The minimum weight of $C$ is defined to be the number $\min \{|f| : f \in C \setminus \{0\}\}$. The dual code $C^\perp$ of $C$ is the orthocomplement of $C$ with respect to $\langle \cdot, \cdot \rangle$. Thus $C^\perp := \{g \in \mathbb{F}_p^P : \langle g, f \rangle = 0, \forall f \in C\}$. The Hamming weight enumerator of $C$ is the polynomial $F \in \mathbb{Z}[X, Y]$ given by $F(X, Y) = \sum_{f \in C} X^{\#(f)} Y^{|f|}$, where $n := \#(P)$ is the so-called length of $C$. If $Z = (Z_\alpha : \alpha \in \mathbb{F}_p)$ is a $p$-tuple of commuting variables, then the complete weight enumerator $G(Z)$ of $C$ is defined to be the polynomial $G(Z) = \sum_{f \in C} Z^{\text{type}(f)}$. Here we have used the usual notation $Z^f$ for $\prod \alpha Z_i^\alpha$, where $i = (i_\alpha : \alpha \in \mathbb{F}_p)$ is a multi-index. Note that the complete weight enumerator (c.w.e.) of $C$ carries much more information about the code than
the Hamming weight enumerator. Indeed, if \( f \) is a word of type \( i \) then the Hamming weight of \( f \) is \( \sum_{a \in \mathbb{F}_p} i_a \). Therefore, \( F \) may be obtained from \( G \) by the substitutions \( X = Z_0, Y = Z_1, Z_2 = \cdots = Z_{p-1} \). The Hamming weight enumerator enumerates the frequencies of various Hamming weights occurring in the code, while the complete weight enumerator enumerates the frequencies of the various types. Finally, note that since \( \langle , \cdot \rangle \) is non-degenerate - we have the usual formula relating the dimensions of \( C \) and \( C^\perp \): \( \dim(C) + \dim(C^\perp) = n \). There are also beautiful formulae giving the Hamming weight enumerator (and, more generally, the c.w.e.) of \( C^\perp \) in terms of the corresponding enumerator of \( C \). While these formulae are extremely important, we shall have no occasion to use them in this paper.

Let \( \mathcal{X} \) be a finite incidence system and \( p \) be a prime. Let \( P \) be the point set of \( \mathcal{X} \). For any line \( \ell \in \mathcal{X} \), we consider its indicator function \( \ell : P \to \mathbb{F}_p \) given by \( \ell(x) = 1 \) if \( x \in \ell \), and \( \ell(x) = 0 \) if \( x \notin \ell \). Note that we have used the same letter to denote a line and its indicator. Thus, lines of \( \mathcal{X} \) are also code words in \( \mathbb{F}_p^P \). The \( p \)-ary code \( C_p(\mathcal{X}) \) of \( \mathcal{X} \) is defined to be the vector subspace of \( \mathbb{F}_p^P \) spanned by all the lines of \( \mathcal{X} \).

If \( p \) is a finite projective plane of order \( n \), then it is easy to see that \( C_p(\pi) \) is trivial when \( p \) does not divide \( n \). However, when \( p \) divides \( n \), \( C_p(\pi) \cap C_p^\perp(\pi) \) is of co-dimension one in \( C_p(\pi) \) (this intersection, the so-called “hull”, is actually spanned by the pairwise differences of the lines of \( \pi \)). Also, when \( p \) divides \( n \), the minimum weight of \( C_p(\pi) \) is \( n + 1 \), and the minimum weight words of \( C_p(\pi) \) are precisely the non-zero scalar multiples of the lines of \( \pi \). When \( p \) exactly divides \( n \) (i.e., \( p \mid n \) but \( p^2 \nmid n \)) \( C_p^\perp(\pi) \) is a subcode (of codimension one) in \( C_p(\pi) \), so that \( \dim(C_p^\perp(\pi)) = \binom{n+1}{2} \) and \( \dim(C_p(\pi)) = \binom{n}{2} + 1 \). See [1, Theorems 4.6.1, 4.6.2, 6.3.1] for the proofs of these results.

In particular, if \( \pi \) is a projective plane of prime order \( p \), \( C_p^\perp(\pi) \subset C_p(\pi) \), \( \dim C_p^\perp(\pi) = \binom{p+1}{2} \), \( \dim C_p(\pi) = \binom{p+1}{2} + 1 \), and the minimum weight words of \( C_p(\pi) \) are the non-zero scalar multiples of lines. Also, Inamdar [10] proved that, in this case, the minimum weight words of \( C_p^\perp(\pi) \) are precisely the non-zero scalar multiples of the pairwise differences of lines of \( \pi \).

These results apply, in particular, to the \( p \)-ary code of \( PG(2, \mathbb{F}_p) \). In [4], the present author proved that the first four minimum weights of the \( p \)-ary code of \( PG(2, \mathbb{F}_p) \) (\( p \geq 5 \)) are \( p + 1, 2p, 2p + 1, \) and \( 3p - 3 \). In an earlier paper [7], Fack et al. had proved that the only words of weight \( p + 1, 2p \) or \( 2p + 1 \) (in this particular code) are the non-zero \( \mathbb{F}_p \)-linear combinations of pairs of lines in \( PG(2, \mathbb{F}_p) \). We shall return to this circle of results in the concluding section of this paper.

The main result of this paper (Theorem 4.2) is that if \( \pi \) is any projective plane of prime order \( p \), and \( \mathcal{X} \) is any partial linear space with at most \( \log_2 p \) lines, then the number of isomorphic copies of \( \mathcal{X} \) in \( \pi \) is determined by the c.w.e. \( G \) of the \( p \)-ary code of \( \pi \). Indeed, this number is given (see Eqs. (3), (6) and (7) in Sect. 4) as an explicit linear combination (with rational coefficients determined by \( p \) and \( \mathcal{X} \)) of the coefficients of \( G \). Choosing \( \mathcal{X} \) to be the configuration of Pappus (which is a special partial linear space with nine lines), it follows (Theorem 4.5) that if \( \pi \) is a projective plane of prime order \( p > 2^9 \), and the \( p \)-ary code of \( \pi \) has the same c.w.e. as that of \( PG(2, \mathbb{F}_p) \), then \( \pi \) must be isomorphic to \( PG(2, \mathbb{F}_p) \). In other words, at least when the prime \( p \) is large, \( PG(2, \mathbb{F}_p) \) is uniquely determined among all projective planes of order \( p \) by its c.w.e. This is a confirmation of the philosophy enunciated in our previous paper [3].
3 A series of Lemmas

In this section we prove a number of lemmas culminating in Lemma 3.9 which will be used in the next section. Our first lemma is well known. For instance, this is an immediate consequence of [1, Theorem 4.6.2] applied to projective planes of prime order.

**Lemma 3.1** Let \( P \) be the point set of a projective plane \( \pi \) of prime order \( p \). Let \( w \in \mathbb{F}_p^P \). Then \( w \in C_p(\pi) \) if and only if \( \langle w, \ell \rangle = \langle w, 1 \rangle \) for all lines \( \ell \) of \( \pi \). (Here 1 is the constant function 1 on \( P \).)

**Proof** This means that \( w \in C_p \) iff \( w \) is orthogonal to all the words in the set \( X = \{1 - \ell : \ell \) a line of \( \pi \}. \) This is true since \( X \) spans \( C_p^\perp \). Indeed, it is clear that the code \( C^0 \) spanned by \( X \) is contained in \( C_p^\perp \) and is of dimension one in \( C_p \). Since \( C_p^\perp \) is of codimension one in \( C_p \) (see [1, Theorem 4.6.2]), it follows that \( C^0 = C_p^\perp \). \( \square \)

**Lemma 3.2** Let \( \mathcal{X} \) be a finite partial linear space and let \( p \) be a prime. Then \( \dim(C_p(\mathcal{X}^*)) = \dim(C_p(\mathcal{X})) \).

**Proof** Let \( \mathcal{X} = (P, L), v = \#(P), b = \#(L) \). Let \( N \) be the \( v \times b \) incidence matrix of \( \mathcal{X} \). That is, the rows and columns of \( N \) are indexed by \( P \) and \( L \) respectively, and the \( (x, \ell) \)th entry of \( N \) is \( 1 \) if \( x \in \ell \) and \( 0 \) otherwise. If we view \( N \) as a linear operator from \( \mathbb{F}_p^L \) to \( \mathbb{F}_p^P \), then \( C_p(\mathcal{X}) \) is precisely the image of \( N \). Therefore \( \dim(C_p(\mathcal{X})) = \text{rank}_p(N) \).

Now note that the transposed matrix \( N^* \) is the incidence matrix of \( \mathcal{X}^* \), so that we also have \( \dim(C_p(\mathcal{X}^*)) = \text{rank}_p(N^*) \). As \( \text{rank}_p(N^*) = \text{rank}_p(N) \), the result follows. \( \square \)

**Lemma 3.3** Let \( \pi \) and \( \sigma \) be two projective planes of order \( n \). Suppose \( \pi \) and \( \sigma \) share at least \( n^2 + 1 \) lines. Then \( \pi = \sigma \).

**Proof** Let \( L_0 \) be a set of \( n^2 + 1 \) lines common to \( \pi \) and \( \sigma \). Since each point of \( \pi \) is in \( n + 1 \) lines, it follows that at least \( n + 1 \) lines need to be removed from \( \pi \) in order to miss a point. Since \( L_0 \) misses only \( n \) lines of \( \pi \), the union of the lines in \( L_0 \) is the entire point set of \( \pi \).

Similarly for \( \sigma \). So \( \pi \) and \( \sigma \) have the same point set, call it \( P \). Fix a prime divisor \( p \) of \( n \). Let \( C_0 \) be the subcode of \( \mathbb{F}_p^P \) spanned by \( L_0 \). Thus \( C_0 \) is a subcode of both \( C_p(\pi) \) and \( C_p(\sigma) \).

Consider the incidence system \( \mathcal{X} = (P, L_0) \). Thus, \( C_0 = C_p(\mathcal{X}) \). Consider the restriction map \( \rho : \mathbb{F}_p^L \rightarrow \mathbb{F}_p^L \) given by \( w \mapsto w |_{L_0} \), where \( L \) is the full set of lines of \( \pi \). \( \rho \) is a linear map which restricts to a linear map from \( C_p(\pi^*) \) onto \( C_p(\mathcal{X}^*) \). The kernel of this restricted map consists of the words \( w \) of \( C_p(\pi^*) \) with support \( w \subseteq L \setminus L_0 \). But \( \#(L \setminus L_0) = n \) and \( C_p(\pi^*) \) has no non-zero word of Hamming weight \( \leq n \) (see [1, Theorem 6.3.1]). Therefore, the kernel is trivial and so \( \rho \) restricts to a vector space isomorphism between \( C_p(\pi^*) \) and \( C_p(\mathcal{X}^*) \). In conjunction with Lemma 3.2, this yields \( \dim(C_p(\pi)) = \dim(C_p(\pi^*)) = \dim(C_p(\sigma)) = \dim(C_p(\mathcal{X})) \).

Since \( C_0 = C_p(\mathcal{X}) \) is a subcode of \( C_p(\pi) \), it follows that \( C_p(\pi) = C_0 \). Similarly, \( C_p(\sigma) = C_0 \). Thus, \( C_p(\pi) = C_p(\sigma) \). But the lines of \( \pi \) are precisely the supports of the minimum weight words of \( C_p(\pi) \) (see [1, Theorem 6.3.1]), and similarly for \( \sigma \). Therefore \( \pi \) and \( \sigma \) have the same set of lines as well. Hence \( \pi = \sigma \). \( \square \)

**Definition 3.4** We shall say that an incidence system \( \mathcal{Y} \) is \( p \)-admissible if it satisfies (i) \( \mathcal{Y} \) has exactly \( p^2 + p + 1 \) points, (ii) each line of \( \mathcal{Y} \) is incident with exactly \( p + 1 \) points, and (iii) any two distinct lines of \( \mathcal{Y} \) are together incident with a unique point.

Thus, any \( p \)-admissible incidence system is a partial linear space. Note that any set of lines in a projective plane of order \( p \) may be viewed as the set of all lines of a \( p \)-admissible incidence system.
Lemma 3.5 Let \( p \geq 2 \). Let \( \sigma \) be a \( p \)-admissible system. Then \( \sigma \) has at most \( p^2 + p + 1 \) lines. Equality holds iff \( \sigma \) is a projective plane of order \( p \).

Proof Fix a point \( x \) of \( \sigma \). Then the lines of \( \sigma \) through \( x \), minus the point \( x \), are pairwise disjoint subsets of size \( p \) each in the set of \( p(p+1) \) remaining points. So each of the \( p^2 + p + 1 \) points \( x \) is in at most \( p + 1 \) lines. But each of the lines of \( \sigma \) contains exactly \( p + 1 \) points.

Now suppose \( \sigma \) has \( p^2 + p + 1 \) lines. Then the above argument shows that each point \( x \) is in exactly \( p + 1 \) lines. Therefore the lines through \( x \) induce a partition of the remaining points. So, if \( y \neq x \) is another point, then a unique line joins \( x \) and \( y \). Since \( x \) was arbitrary, this shows that any two distinct points of \( \sigma \) are together in a unique line of \( \sigma \).

Now fix two lines \( \ell_1 \neq \ell_2 \) of \( \sigma \). Since \( \#(\ell_1 \cup \ell_2) = 2p + 1 < p^2 + p + 1 \), there is a point non-incident with both \( \ell_1 \) and \( \ell_2 \). So \( \sigma \) is a projective plane of order \( p \).

Lemma 3.6 Let \( S \) be the union of \( k \geq 1 \) lines of a \( p \)-admissible incidence system. Then \((p + 1)k - \binom{k}{2} \leq \#(S) \leq pk + 1\).

Proof Induction on \( k \). The result is trivial for \( k = 1 \). So let \( k > 1 \), and let \( S = \bigcup_{0 \leq i < k} \ell_i \), where \( \ell_i \)'s are distinct lines of the \( p \)-admissible incidence system. Write \( S = S' \cup \ell_{k-1} \), where \( S' = \bigcup_{0 \leq i < k-1} \ell_i \).

Since any two distinct lines meet at a unique point, we have \( 1 \leq \#(S' \cap \ell_{k-1}) \leq k - 1 \). Since, also, each line is of size \( p + 1 \), we get

\[
k(p + 1) - \binom{k}{2} = (k - 1)(p + 1) - \binom{k - 1}{2} + (p + 1) - (k - 1)\]

\[
\leq \#(S') + \#(\ell_{k-1}) - \#(S' \cap \ell_{k-1})\]

\[
\leq (k - 1)p + 1 + (p + 1) - 1 \]

\[
= kp + 1.
\]

As \( \#(S') + \#(\ell_{k-1}) - \#(S' \cap \ell_{k-1}) = \#(S) \), this completes induction.

Lemma 3.7 Let \( \mathcal{Y} \) and \( \mathcal{Y}' \) be two \( p \)-admissible incidence systems. Suppose the union of some \( m \) lines of \( \mathcal{Y} \) equals the union of some \( k \) lines of \( \mathcal{Y}' \). If \( \binom{k}{2} < p \) then \( m = k \).

Proof Let \( S \) be a set which is the union of \( m \) lines of \( \mathcal{Y} \) as well as the union of \( k \) lines of \( \mathcal{Y}' \). Since \( p > \binom{k}{2} \), Lemma 3.6 implies that \((k - 1)p + 1 < (p + 1)(k - \binom{k}{2}) \leq \#(S) \leq mp + 1\). Therefore \( m \geq k \). Suppose, in order to derive a contradiction, that \( m > k \). Then \( S \) is the union of \( k \) lines of \( \mathcal{Y}' \) and \( S \) contains the union of \( k + 1 \) lines of \( \mathcal{Y} \). Therefore, Lemma 3.6 implies that we have \((k + 1)(p + 1) - \binom{k + 1}{2} \leq \#(S) \leq kp + 1\). Hence \( p \leq \binom{k}{2} \). But this contradicts our assumption.

The next lemma is actually a special case of the following general observation:- among all partitions of a positive integer into powers of two, its binary expansion (i.e., the partition into distinct parts) is the only one with the fewest parts. This lemma is one of the two key tools in the proof of Lemma 3.9. The second tool is two-way counting argument.

Lemma 3.8 Let \( k \) be a positive integer, and let \( x_i, 0 \leq i < k \), be \( k \) non-negative integers such that \( \sum_{0 \leq i < k} 2^i x_i = 2^k - 1 \). Then,

\[
(a) \quad \sum_{0 \leq i < k} x_i \geq k, \text{ and}
\]
(b) if $\sum_{0 \leq i < k} x_i = k$ then $x_i = 1$ for all $i$.

**Proof** It suffices to show that if $\sum_{0 \leq i < k} x_i \leq k$ then $x_i = 1$ for all $i$. We prove this by induction on $k$. The result is trivial for $k = 1$. So assume $k > 1$. Note that $\sum_{0 \leq i < k} 2^i x_i = 2^k - 1$ implies that $x_0$ is odd. In particular, $x_0 \geq 1$. We define $k - 1$ non-negative integers $y_i$, $0 \leq i < k - 1$, as follows. $y_0 = \frac{1}{2}(x_0 - 1) + x_1$, and $y_i = x_{i+1}$ for $1 \leq i < k - 1$. We have $\sum_{0 \leq i < k - 1} 2^i y_i = \frac{1}{2}(1 - 1 + \sum_{0 \leq i < k} 2^i x_i) = 2^{k-1} - 1$, and $\sum_{0 \leq i < k - 1} y_i < \sum_{0 \leq i < k} x_i \leq k$. Therefore, the induction hypothesis implies that $y_i = 1$ for $0 \leq i < k - 1$. That is, $x_i = 1$ for $1 < i < k$, and $x_0 + 2x_1 = 3$. So, either $x_0 = x_1 = 1$, or $x_0 = 3, x_1 = 0$. But, in the latter case, we get $\sum_{0 \leq i < k} x_i = k + 1$, contrary to our assumption. So $x_i = 1$ for all $i$. This completes induction. \qed

**Lemma 3.9** Let $p$ be a prime, and $\mathcal{Y}$ be a $p$-admissible incidence system with exactly $k$ lines. Enumerate the lines of $\mathcal{Y}$ (in any order) as $\ell_i$, $0 \leq i < k$. Consider the word $w \in C_p(\mathcal{Y})$ given by $w = \sum_{0 \leq i < k} 2^i \ell_i$. Let $\pi$ be a projective plane of order $p$, and suppose $w'$ is a word in $C_p(\pi)$ such that type($w'$) = type($w$). If $p \geq 2^k$, then there are lines $\ell'_i$, $0 \leq i < k$, of $\pi$ such that $w' = \sum_{0 \leq i < k} 2^i \ell'_i$. Further, there is a monomorphism $f$ from $\mathcal{Y}$ into $\pi$ such that $f(\ell_i) = \ell'_i$, $0 \leq i < k$. Indeed, any bijection $f$ satisfying $w' = w \circ f^{-1}$ is such a monomorphism.

**Proof** For integers $i \geq 0$ and $x \geq 0$, let $\delta_i(x)$ denote the $i$th digit in the binary expansion of $x$. That is, if $\sum_{i \geq 0} a_i 2^i$ is the binary expansion of $x$ (so that each $a_i = 0$ or 1, and all but finitely many $a_i$’s are 0), then $\delta_i(x) = a_i$.

Let $P$ and $Q$ be the point sets of $\pi$ and $\mathcal{Y}$, respectively. For $0 \leq i < k$, define

$$\ell'_i = \{x \in P : \delta_i(w'(x)) = 1\}.$$

(Here we have identified the elements of $F_p$ with the integers 0, 1, ..., $p - 1$.) Notice that, since $w = \sum_{0 \leq i < k} 2^i \ell_i$, and $p \geq 2^k$, we also have

$$\ell_i = \{x \in Q : \delta_i(w(x)) = 1\}$$

for $0 \leq i < k$. Further, by the definition of $\ell'_i$, we have

$$w' = \sum_{0 \leq i < k} 2^i \ell'_i.$$

As type($w'$) = type($w$), there is a bijection $f : Q \rightarrow P$ such that $w' = w \circ f^{-1}$. It follows that for $x \in Q$, and $0 \leq i < k$,

$$x \in \ell_i \Leftrightarrow \delta_i(w(x)) = 1 \Leftrightarrow \delta_i(w'(f(x))) = 1 \Leftrightarrow f(x) \in \ell'_i.$$

Thus $f(\ell_i) = \ell'_i$, for $0 \leq i < k$. Therefore, if $\mathcal{Y}'$ denotes the incidence system with point set $P$ and lines $\ell'_i$, $0 \leq i < k$, then $f$ is an isomorphism between $\mathcal{Y}$ and $\mathcal{Y}'$. In consequence, $\mathcal{Y}'$ is also $p$-admissible, so that $\ell'_i$ are sets of size $p + 1$ each, and any two distinct $\ell'_i$’s meet at a unique point.

Thus, to complete the proof, we have to show that the $k$ sets $\ell'_i$ are lines of $\pi$. So far we have not used the assumption $w' \in C_p(\pi)$. This assumption will play a crucial role in what follows.

Let $S$ and $S'$ be the supports of $w$ and $w'$ respectively. Since $p \geq 2^k$, we have $S = \bigcup_{0 \leq i < k} \ell_i$ and $S' = \bigcup_{0 \leq i < k} \ell'_i$. \((\mathcal{S})\) Springer
Claim 1 If \( \ell \) is a line of \( \pi \) such that \( \ell \not\subseteq S' \), then \( \sum_{x \in \ell} w'(x) = 2^k - 1 \) (equality in \( \mathbb{N} \)). To prove this claim, first we note that

\[
\sum_{x \in P} w'(x) \equiv \langle w', 1 \rangle \equiv \langle w, 1 \rangle \equiv \left( \sum_{0 \leq i < k} 2^i \ell_i, 1 \right) \equiv \sum_{0 \leq i < k} 2^i \equiv 2^k - 1 \text{(mod } p). \]

Since \( w' \in C_\ell(\pi) \), Lemma 3.1 implies that \( \sum_{x \in \ell} w'(x) \equiv 2^k - 1 \text{(mod } p) \) for any line \( \ell \) of \( \pi \). Therefore we have, as \( p \geq 2^k \),

\[
\sum_{x \in \ell} w'(x) \geq 2^k - 1 \tag{1}
\]

for any line \( \ell \) of \( \pi \) (inequality in \( \mathbb{N} \)).

Now fix a point \( y \not\in S' \). Adding the inequalities (1) over all the \( p + 1 \) lines \( \ell \) through \( y \), we get

\[
(p + 1)(2^k - 1) \leq \sum_{\ell \ni y} \sum_{x \in \ell} w'(x) = \sum_{x \in P} w'(x) = \sum_{x \in P} \sum_{0 \leq i < k} 2^i \ell_i(x) = \sum_{0 \leq i < k} \sum_{x \in P} 2^i \ell_i(x) = (p + 1)(2^k - 1).
\]

Since the two extreme terms here are equal, we must have equality throughout this argument. Therefore we have equality in (1) for any line \( \ell \) through \( y \). Since \( y \not\in S' \) was an arbitrary point, we have equality for any line \( \ell \not\subseteq S' \). This proves Claim 1.

Claim 2 For any line \( \ell \not\subseteq S' \) of \( \pi \), we have \#(\( \ell \cap \ell_i' \)) = 1 for 0 \( \leq i < k \).

To prove this claim, note that

\[
\sum_{0 \leq i < k} 2^i \#(\ell \cap \ell_i') = \sum_{x \in \ell} \sum_{0 \leq i < k} 2^i \ell_i'(x) = \sum_{x \in \ell} w'(x) = 2^k - 1 \text{(by Claim 1)}.
\]

Therefore, Lemma 3.8 (a) implies that

\[
\sum_{0 \leq i < k} \#(\ell \cap \ell_i') \geq k \tag{2}
\]

for any line \( \ell \not\subseteq S' \).
Again, fix a point \( y \notin S' \), and add the inequality (2) over all \( p + 1 \) lines \( \ell \) of \( \pi \) through \( y \). We get:

\[
(p + 1)k \leq \sum_{\ell \ni y} \sum_{0 \leq i < k} \#(\ell \cap \ell'_i) \\
= \sum_{0 \leq i < k} \sum_{\ell \ni y} \#(\ell \cap \ell'_i) \\
= \sum_{0 \leq i < k} \#(\ell'_i) \\
= (p + 1)k.
\]

Since the two extreme terms here are equal, we must have equality throughout this argument. Thus, we have equality in (2) for any line \( \ell \) through \( y \). Since the point \( y \notin S' \) was arbitrary, it follows that we have equality in (2) for any line \( \ell \notin S' \). Therefore Lemma 3.8 (b) implies that \( \#(\ell \cap \ell'_i) = 1 \), for \( 0 \leq i < k \) and for any such line \( \ell \). This proves Claim 2.

**Claim 3** \( S' \) contains exactly \( k \) lines of \( \pi \).

To see this, let \( m \) be the number of lines \( \ell \) of \( \pi \) such that \( \ell \subseteq S' \). Since \( S' \) is the union of the sets \( \ell'_i \), \( 0 \leq i < k \), and since, by Claim 2, for any two points \( x \neq y \) in \( \ell'_i \) the line \( \ell \) of \( \pi \) joining \( x \) and \( y \) is contained in \( S' \), it follows that \( S' \) is the union of \( m \) lines of \( \pi \), as well as the union of \( k \) lines of \( S' \). Since \( p \geq 2^k > \left(\frac{k}{2}\right) \), Lemma 3.7 implies that \( m = k \). This proves Claim 3.

Now, let \( \sigma \) be the incidence system obtained from \( \pi \) by deleting the \( k \) lines contained in \( S' \) and replacing them by the \( k \) lines of \( S' \) (contained in \( S' \)). Since \( \pi \) is a projective plane of order \( p \) and \( S' \) is \( p \)-admissible, Claim 2 implies that \( \sigma \) is \( p \)-admissible. Since \( \sigma \) has \( p^2 + p + 1 \) lines, Lemma 3.5 implies that \( \sigma \) is also a projective plane of order \( p \). Also, by construction, \( \sigma \) and \( \pi \) share at least \( p^2 + p + 1 - k \geq p^2 + p + 1 - \log_2 p \geq p^2 + 1 \) lines. Therefore, by Lemma 3.3, \( \sigma = \pi \). Since \( \ell'_i \) (\( 0 \leq i < k \)) are lines of \( \sigma \), it follows that they are lines of \( \pi \). \( \square \)

### 4 The main results

We now introduce:

**Notation** Let \( \mathcal{Y} \) and \( \mathcal{X} \) be any two finite partial linear spaces. Then \( I(\mathcal{Y}, \mathcal{X}) \) will denote the number of monomorphisms from \( \mathcal{Y} \) into \( \mathcal{X} \). Also, \( i(\mathcal{Y}, \mathcal{X}) \) will denote the number of isomorphic copies of \( \mathcal{Y} \) which are subsystems of \( \mathcal{X} \).

**Lemma 4.1** For any two finite partial linear spaces \( \mathcal{Y} \) and \( \mathcal{X} \), we have \( I(\mathcal{Y}, \mathcal{X}) = \#(\text{Aut}(\mathcal{Y})) \cdot i(\mathcal{Y}, \mathcal{X}) \).

**Proof** Note that, for any monomorphism \( f \) from \( \mathcal{Y} \) to \( \mathcal{X} \), the image \( \mathcal{Y}' \) of \( \mathcal{Y} \) under \( f \) is an isomorphic copy of \( \mathcal{Y} \) in \( \mathcal{X} \), and \( f \) may be viewed as an isomorphism from \( \mathcal{Y} \) to \( \mathcal{Y}' \). Conversely, for any isomorphic copy \( \mathcal{Y}' \) of \( \mathcal{Y} \) in \( \mathcal{X} \), any isomorphism from \( \mathcal{Y} \) to \( \mathcal{Y}' \) may be viewed as a monomorphism from \( \mathcal{Y} \) to \( \mathcal{X} \). Therefore, to complete the proof, it suffices to show that, whenever \( \mathcal{Y} \) and \( \mathcal{Y}' \) are isomorphic finite partial linear spaces, the number of isomorphisms from \( \mathcal{Y} \) to \( \mathcal{Y}' \) equals \( \#(\text{Aut}(\mathcal{Y})) \). To see this, fix any isomorphism \( f \) from \( \mathcal{Y} \) to \( \mathcal{Y}' \), and note that \( g \mapsto f \circ g \) is a bijection from the set of all automorphisms of \( \mathcal{Y} \) onto the set of all isomorphisms from \( \mathcal{Y} \) to \( \mathcal{Y}' \). \( \square \)
Notation For any prime $p$, let $\mathcal{J}_p$ denote the set of all multi-indices $\underline{j} = (j_\alpha : \alpha \in \mathbb{F}_p)$ such that $|\underline{j}| := \sum_{\alpha \in \mathbb{F}_p} j_\alpha = p^2 + p + 1$. Also, let $\mathcal{X} = (X_\alpha : \alpha \in \mathbb{F}_p)$ be a set of commuting variables.

**Theorem 4.2** Let $\pi$ be a projective plane of prime order $p$, and let $G(X) = \sum_{\underline{i} \in \mathcal{J}_p} a_{\underline{i}} X_{\underline{i}}$ be the complete weight enumerator of $C_p(\pi)$. (Thus, for $\underline{i} \in \mathcal{J}_p$, $a_{\underline{i}}$ is the number of words of type $\underline{i}$ in $C_p(\pi)$.) Then, for any partial linear space $\mathcal{X}$ with at most $\log_2 p$ lines, there are rational numbers $\alpha_{\underline{i}}$, $\underline{i} \in \mathcal{J}_p$, depending only on $\mathcal{X}$ and $p$, such that $\underline{i}(\mathcal{X}, \pi) = \sum_{\underline{i} \in \mathcal{J}_p} a_{\underline{i}} \alpha_{\underline{i}}$.}

**Proof** We first prove this result in the case of $p$-admissible incidence systems. So let $\mathcal{Y}$ be a $p$-admissible incidence system with, say, $k \leq \log_2 p$ lines. Choose and fix an ordering of the lines of $\mathcal{Y}$. Let $\underline{j} = \underline{j}(\mathcal{Y})$ be the type of the word $w \in C_p(\mathcal{Y})$ given in Lemma 3.9. For each of the $a_{\underline{i}}$ words $w'$ in $C_p(\pi)$ of type $\underline{i}$, clearly there are exactly $j_\pi! := \prod_{\alpha} j_\alpha!$ bijections $f$ from the point set of $\mathcal{Y}$ to the point set of $\mathcal{X}$ such that $f' = w \circ f^{-1}$. By Lemma 3.9, all these bijections $f$ are monomorphisms from $\mathcal{Y}$ into $\pi$. On the other hand, for any of the $I(\mathcal{Y}, \pi)$ monomorphisms $f$ from $\mathcal{Y}$ into $\pi$, $f' = w \circ f^{-1}$ is clearly a word of $C_p(\pi)$ of type $j$. Therefore, a two-way counting argument yields $I(\mathcal{Y}, \pi) = \underline{j}! a_{\underline{j}}$. Therefore, by Lemma 4.1,

$$\underline{i}(\mathcal{Y}, \pi) = \frac{\underline{j}! a_{\underline{j}}}{\#(\operatorname{Aut}(\mathcal{Y}))}.$$ 

For any $\underline{i} \in \mathcal{J}_p$, let’s put

$$\beta_{\underline{i}}(\mathcal{Y}) = \begin{cases} \frac{\underline{i}!}{\#(\operatorname{Aut}(\mathcal{Y}))} & \text{if } \underline{i} = \underline{j}(\mathcal{Y}) \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Then the formula for $\underline{i}(\mathcal{Y}, \pi)$ may be rewritten as:

$$\underline{i}(\mathcal{Y}, \pi) = \sum_{\underline{i} \in \mathcal{J}_p} \beta_{\underline{i}}(\mathcal{Y}) a_{\underline{i}} \tag{4}$$

for all $p$-admissible incidence systems $\mathcal{Y}$ with $k \leq \log_2 p$ lines. This proves the theorem in the case of $p$-admissible systems.

Now let $\mathcal{X}$ be an arbitrary partial linear space with, say, $k \leq \log_2 p$ lines. Note that, for any positive integer $v$, up to isomorphism there are only finitely many incidence systems with $v$ points. Indeed, w.l.o.g., the point set of any such system may be taken to be the set $\{1, 2, \ldots, v\}$. A fortiori, there are, up to isomorphism, only finitely many $p$-admissible incidence systems $\mathcal{Y}$ (for the given $p$) with $k$ lines. Let $A_{k,p}$ denote a complete (finite) list of all such pairwise non-isomorphic systems $\mathcal{Y}$. For any isomorphic copy $\mathcal{X}'$ of $\mathcal{X}$ in $\pi$, and any line $\ell'$ of $\mathcal{X}'$, let $\tilde{\ell}$ denote the unique line of $\pi$ containing $\ell$. Let $\mathcal{Y}'$ be the incidence system whose lines are these lines $\tilde{\ell}$ as $\ell'$ varies over the lines of $\mathcal{X}'$. Clearly $\mathcal{Y}'$ is the unique $p$-admissible incidence system with $k$ lines sandwiched between $\mathcal{X}'$ and $\pi$. There is a unique system $\mathcal{Y}$ in $A_{k,p}$ such that $\mathcal{Y}$ is isomorphic to $\mathcal{Y}'$. This proves that, for any of the $\underline{i}(\mathcal{X}, \pi)$ copies $\mathcal{X}'$ of $\mathcal{X}$ in $\pi$, there is a unique $\mathcal{Y}$ in $A_{k,p}$ and a unique isomorphic copy $\mathcal{Y}'$ of $\mathcal{Y}$, such that $\mathcal{Y}'$ lies between $\mathcal{X}'$ and $\pi$. On the other hand, for any $\mathcal{Y}$ in $A_{k,p}$, and any of the $\underline{i}(\mathcal{Y}, \pi)$ isomorphic copies $\mathcal{Y}'$ of $\mathcal{Y}$ in $\pi$, there are exactly $\underline{i}(\mathcal{X}', \mathcal{Y}') = \underline{i}(\mathcal{X}, \mathcal{Y})$ isomorphic copies $\mathcal{X}'$ of $\mathcal{X}$ such that $\mathcal{Y}'$ is between $\mathcal{X}'$ and $\pi$. Therefore, a two-way counting yields:

$$\underline{i}(\mathcal{X}, \pi) = \sum_{\mathcal{Y}} \underline{i}(\mathcal{X}, \mathcal{Y}) \underline{i}(\mathcal{Y}, \pi) \tag{5}$$

where the sum is over all $\mathcal{Y}$ in the finite list $A_{k,p}$.
Substituting the formula (4) into (5), we get

$$i(X, \pi) = \sum_{i \in J_p} \alpha_i a_{i}$$

(6)

where, for $i \in J_p$,

$$\alpha_i = \alpha_{i}(X) = \sum_{Y} i(X', Y) \beta_i(Y).$$

(7)

Here, again, the sum is over all $Y$ in $A_k p$, and $\beta_i(Y)$ is given by the formula (3). The formula (6) gives the required expression of $i(X, \pi)$ as a rational linear combination of the coefficients of $G$. \hfill \Box

As an immediate consequence of Theorem 4.2, we have:

**Corollary 4.3** Let $\pi, \sigma$ be two projective planes of prime order $p$. Suppose $C_p(\pi)$ and $C_p(\sigma)$ have the same complete weight enumerator. Then, for any partial linear space $X$ with at most $\log_2 p$ lines, we have $i(X, \pi) = i(X, \sigma)$.

**Theorem of Pappus** Let $\{x_1, x_2, x_3\}$ and $\{y_1, y_2, y_3\}$ be two disjoint 3-sets of collinear points of a projective plane $\pi$. Suppose $\{x_1, x_2, x_3\}$ and $\{y_1, y_2, y_3\}$ determine two distinct lines $\ell_1, \ell_2$ of $\pi$ and the six points $x_i, y_i$ $(1 \leq i \leq 3)$ are distinct from the point $\ell_1 \cap \ell_2$. Let us put

$$z_1 = (x_2 \lor y_3) \land (x_3 \lor y_2),$$

$$z_2 = (x_1 \lor y_3) \land (x_3 \lor y_1),$$

$$z_3 = (x_1 \lor y_2) \land (x_2 \lor y_1).$$

We say that the theorem of Pappus holds in $\pi$, or that $\pi$ is a Pappian plane, if, for every such choice of six initial points $x_i, y_i$ $(1 \leq i \leq 3)$ in $\pi$, the three points $z_1, z_2, z_3$ are collinear in $\pi$. ([5, p. 158] and [9, pp. 25–26]).

A projective plane need not be Pappian. In fact, a famous theorem in Projective Geometry states that a projective plane $\pi$ is Pappian iff $\pi$ is the projective plane over a field. This follows from the result in [9, p. 159] and Hilbert’s theorem quoted below.

It is easy to see that the nine points $x_i, y_i, z_i$ $(1 \leq i \leq 3)$ occurring in Pappus’ theorem are necessarily distinct. When Pappus’ theorem holds, this set of nine points contains the nine collinear triples listed in Table 1. For some initial choices of the six points $x_i, y_i$, some or all of the three triples $\{x_i, y_i, z_i\}$, $1 \leq i \leq 3$, may also be collinear. But this does not affect the following arguments.

Consider the partial linear space $P$ with nine points and nine lines which is the subsystem of $PG(2, F_3)$ obtained as follows. Fix a flag (i.e., an incident point-line pair) $(x, \ell)$ in $PG(2, F_3)$. Then $P$ is the subsystem of $PG(2, F_3)$ whose points are the points of $PG(2, F_3)$ non-incident with $\ell$, and whose lines are the intersections with this point set of the lines of $PG(2, F_3)$ non-incident with $x$. Since the automorphism group of $PG(2, F_3)$ is transitive on the flags, this defines the partial linear space $P$ uniquely up to isomorphism.

Springer
Note that the nine collinear triples of Table 1, occurring in the “Theorem of Pappus”, form an explicit list of the lines of \( \mathbb{P} \). This is why \( \mathbb{P} \) is sometimes called the **Configuration of Pappus**. (“Configuration” is an old term for a partial linear space.)

Also observe that, despite appearances, the validity (or otherwise) of the “Theorem of Pappus” does not depend on the explicit ordering of the six initial points, but it depends only on the bijection \( x_i \mapsto y_i \) \((1 \leq i \leq 3)\) between the initial collinear tuples \( \{x_1, x_2, x_3\} \) and \( \{y_1, y_2, y_3\} \). More precisely, if the three indices 1, 2, 3 in the statement are consistently permuted, then the validity (or invalidity) of the hypothesis and conclusion of this “theorem” remains unchanged.

In view of these observations, the theorem of Pappus may be reformulated as follows.

**The theorem of Pappus** (alternative version) Let’s say two 3-sets \( \alpha, \beta \) of points in a projective plane \( \pi \) form an **admissible pair** if (i) \( \alpha \) and \( \beta \) are collinear triples, (ii) \( \alpha \) and \( \beta \) are disjoint, and (iii) no four points in \( \alpha \cup \beta \) are collinear in \( \pi \). Then \( \pi \) is said to satisfy the “theorem of Pappus” or we say that \( \pi \) is Pappian, if, for every pair \( (\alpha, \beta) \) of admissible triples of \( \pi \) and every bijection \( f : \alpha \rightarrow \beta \), there is a unique isomorphic copy of \( \mathbb{P} \) in \( \pi \) such that (a) \( \alpha \) and \( \beta \) are lines of \( \mathbb{P} \), (b) for each \( x \in \alpha \), \( x \) and \( f(x) \) are non-collinear in \( \mathbb{P} \).

Finally, note that the points and lines of \( \mathbb{P} \) are uniquely determined by the triple \((\alpha, \beta, f)\) as above. Namely, the nine points and eight of the lines of \( \mathbb{P} \) are determined by the hypothesis, and the ninth line of \( \mathbb{P} \) is determined by the conclusion of Pappus’ Theorem, given \((\alpha, \beta, f)\).

Therefore, the characterization of finite field planes as the finite Pappian projective planes may be rephrased as follows.

**Theorem 4.4** Let \( \pi \) be a projective plane of order \( n \). Then \( \mathfrak{i}(\mathbb{P}, \pi) \leq \frac{2}{3} (\frac{n^2+n+1}{2}) \binom{n}{3}^2 \). Equality holds here if \( \pi \) is a field plane.

**Proof** Clearly \( \pi \) contains exactly \( 2\binom{n^2+n+1}{2} \binom{n}{3}^2 \) admissible pairs \( (\alpha, \beta) \) of collinear triples. For each such pair, there are 3! bijections \( f : \alpha \rightarrow \beta \). Thus there are \( 12\binom{n^2+n+1}{2} \binom{n}{3}^2 \) triples \( (\alpha, \beta, f) \) as above. Each such triple determines at most one isomorphic copy of \( \mathbb{P} \) in \( \pi \). On the other hand, it is easy to verify that \( \mathbb{P} \) contains exactly 18 ordered pairs \( (\alpha, \beta) \) of disjoint lines, and, for each such pair, there is a unique bijection \( f : \alpha \rightarrow \beta \) such that \( x \) and \( f(x) \) are non-collinear in \( \mathbb{P} \) for all \( x \in \alpha \). Thus, each of the \( \mathfrak{i}(\mathbb{P}, \pi) \) subsystems of \( \pi \) isomorphic to \( \mathbb{P} \) is determined by exactly 18 triples \( (\alpha, \beta, f) \). Therefore, a two-way counting argument yields that \( 18\mathfrak{i}(\mathbb{P}, \pi) \leq 12\binom{n^2+n+1}{2} \binom{n}{3}^2 \), with equality iff \( \pi \) is Pappian. \( \square \)

Using Theorem 4.4 and Corollary 4.3 with \( \mathcal{X} = \mathbb{P}, \sigma = PG(2, \mathbb{F}_p) \), we get (as \( \mathbb{P} \) has nine lines):

**Theorem 4.5** Let \( \pi \) be a projective plane of prime order \( p \) such that \( \pi \) has the same complete weight enumerator (of its \( p \)-ary code) as \( PG(2, \mathbb{F}_p) \). If \( p > 2^9 \), then \( \pi \) is isomorphic to \( PG(2, \mathbb{F}_p) \).

Recall that a projective plane \( \pi \) is said to be **Desarguesian** if (in the standard terminology of projective geometry) each pair of triangles in \( \pi \) which is centrally perspective is also axially perspective (see [5, p. 26]). Consider the Petersen graph, which may be described as the graph whose vertices are the \( \binom{5}{2} \) unordered pairs of symbols from a set of five symbols, with disjointness as adjacency. Let \( D \) be the partial linear space whose points and lines are both indexed by the vertices of the Petersen graph, such that the line indexed by \( x \) is incident with the point indexed by \( y \) if \( x \) and \( y \) are adjacent vertices of the graph. \( D \) is known as the **Configuration of Desargue** (see [9, pp. 105–106]) since it stands in the same relation
with “Desargue’s theorem” as \( \mathbb{P} \) with the “theorem of Pappus”. Therefore, the well-known theorem (this theorem is due to Hilbert, see [5, p. 28]) that a projective plane is a plane over a division ring iff it is desarguesian may be rephrased as in Theorem 4.4 in the finite case. Namely, for every projective plane \( \pi \) of order \( n \), one may write down an upper bound for \( i(D, \pi) \) in terms of \( n \) alone, which is attained iff \( \pi \) is a field plane. Using this theorem, one can write an alternative proof of Theorem 4.5. However, since \( D \) has ten lines, this alternative proof works only for \( p > 2^{10} \). We have chosen to work with \( \mathbb{P} \) since it has fewer lines.

5 Speculations

The bound \( \log_2 p \) in Theorem 4.2 is perhaps the best possible. However, we expect that the bound \( p > 2^6 \) in Theorem 4.5 is unnecessary, and this theorem actually holds for all primes \( p \). For instance, if Conjecture 1.3 is correct, then we can use \( PG(2, \mathbb{F}_2) \) instead of \( \mathbb{P} \) in the proof of Theorem 4.5, pushing its bound to \( p > 2^7 \). In any case, Theorem 4.5 shows that, in order to prove Conjecture 1.2, at least for large primes \( p \), it suffices to calculate the complete weight enumerator for arbitrary projective planes of order \( p \). But this is a tall order! We do not even know the complete weight enumerator of \( PG(2, \mathbb{F}_p) \) for any prime \( p \geq 7 \).

To prove that the fourth minimum weight of the \( p \)-ary code of \( PG(2, \mathbb{F}_p) \) is \( 3p - 3 \), we constructed \((3,4)\) \( p^2(p^3 - 1)\left(\frac{p+1}{3}\right) \) words of weight \( 3p - 3 \) in this code. These words are actually in the dual code. In [2,3] we posed

**Conjecture 5.1** For any projective plane \( \pi \) of prime order \( p \), \( C_{p}^{\perp}(\pi) \) has at most \( p^2(p^3 - 1)\left(\frac{p+1}{3}\right) \) words of Hamming weight \( 3p - 3 \). Equality holds iff \( \pi \) is isomorphic to \( PG(2, \mathbb{F}_p) \).

If this conjecture is correct, then, of course, to prove Conjecture 1.2 it will suffice to investigate the initial segment of the Hamming weight enumerator of the dual \( p \)-ary code of arbitrary projective planes of order \( p \). For \( p > 17 \), the “if” part of Conjecture 5.1 was recently proved in [12, Theorem 4.8]. In fact, they proved that the words mentioned are the only words of weight \( 3p - 3 \) in the larger code \( C_p(PG(2, \mathbb{F}_p)) \).

**Acknowledgements** I thank the referees for their careful reading of the first version of this paper, and particularly for their detailed comments which helped improve the presentation significantly. My heart felt thanks are due to Asha Lata for her efficient and unstinting secretarial help in preparing my papers during my 28 years in the Bangalore Centre of Indian Statistical Institute. All good things in life come to an end. My 48 years long career in the Indian Statistical Institute is now drawing to a close. I wish to thank all my colleagues in I.S.I. for providing me with a relaxed and friendly atmosphere in which to do mathematics.

**References**

1. Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).
2. Bagchi B.: A conjecture on linear spaces of prime order. J. Comb. Inf. Syst. Sci. **34**, 23–31 (2009).
3. Bagchi B.: On characterizing designs by their codes. In: Sastry N.S.N. (ed.) Buildings, Finite Geometries and Groups, vol. 10. Springer Proceedings in MathematicsSpringer, New York (2012).
4. Bagchi, B.: The fourth smallest Hamming weight in the code of the projective plane over \( \mathbb{Z}/p\mathbb{Z} \). http://arxiv.org/abs/1712.07391.
5. Dembowski P.: Finite Geometries. Springer, Berlin (1997).
6. Euler L.: Recherches sur une nouvelle espece des quarres magiques. Verh. Zeeuwsch. Genootsch. Wetensch. Vlissingen **9**, 85–239 (1782).
7. Fack V., Fancsali S.L., Storme L., van de Voorde G., Winne J.: Small weight code words in the codes arising from Desarguasian projective planes. Des. Codes Cryptogr. **46**, 25–43 (2008).
8. Fano G.: Sui postulati fondamentali della geometria proiettiva. Giornale di Matematiche 30, 106–132 (1892).
9. Hughes D.R., Piper F.C.: Projective Planes. Springer, New York (1973).
10. Inamdar S.P.: Rigidity theorems for partial linear spaces. J. Comb. Theory (Ser. A) 96, 388–395 (2001).
11. Neumann H.: On some finite non-desarguesian planes. Arch. Math. 6, 36–40 (1955).
12. Szonyi T., Weiner Z.: Stability of $k \mod p$ multisets and small weight codewords in the code generated by the lines of $PG(2, q)$. J. Comb. Theory (Ser. A) 157, 321–333 (2018).
13. Veblen O., Wedderburn J.H.M.: Non-Desarguesian and non-Pascalian geometries. Trans. Am. Math. Soc. 8, 379–388 (1907).
14. von Staudt G.K.C.: Beiträge zur geometrie der lage 1 (1856).

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.