ELSEVIER

Journal of Statistical Planning and Inference 62 (1997) 3–11

journal of statistical planning and inference

Intersection-sets in $\mathbb{P}G(n,2)$[1]

Aiden Bruen[a], Lucien Haddad[b], David Wehlau[b,c,*]

[a] *Department of Mathematics, University of Western Ontario, London, Ont., Canada N6A 3K7*

[b] *Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, Ont., Canada K7K 5l0*

[c] *Department of Mathematics and Statistics, Queens University, Kingston, Ont., Canada K7L 3N6*

Received 27 May 1994; revised 20 March 1995

Abstract

We want to examine line-free subsets of projective spaces over GF(2) especially from an intersection-set point of view. In this paper, we describe incidence equations for such sets. For every $n\geqslant 3$, we construct a line-free subset (or cap), X_n of $\mathbb{P}G(n,2)$, which meets every hyperplane in at least 2^{n-3} points. We make use of the incidence equations and other methods to show that, remarkably, up to isomorphism, the set X_n is the *unique* set having these two properties for $n = 3,4,5$. The cases $n = 3,4$ are small enough to handle directly. The result for $n = 5$ was in fact established in Fugère et al. (*J. Combin. Designs* **2** (5) (1994) 287–299) using a labourious, detailed case by case analysis. One of the motivations for that result was to decide the chromatic number of $\mathbb{P}G(5,2)$. We also establish various sporadic results on r-intersection-sets in $\mathbb{P}G(n,2)$ when $n = 5,6$.

AMS classification: primary 51 E 15; secondary 05 B 10

Keywords: Caps; Codes; Projective geometry; Blocking sets

1. Definitions and notation

For $n\geqslant 2$, we denote by $\mathbb{P}G(n,2)$ the finite projective space of dimension n over $\mathbb{F} := \mathrm{GF}(2)$, the field of order 2. We can construct $\mathbb{P}G(n,2)$ as follows. Let $\mathbb{F}^{n+1}$ denote the $(n+1)$-dimensional vector space over $\mathbb{F} := \mathrm{GF}(2)$. The elements (or points) of $\mathbb{P}G(n,2)$ are the one-dimensional subspaces of $\mathbb{F}^{n+1}$. Each such subspace is represented by the nonzero vector contained in it. For ease of notation, if $\{e_0,\dots,e_n\}$ is a basis of $\mathbb{F}^{n+1}$ and x is an element of $\mathbb{P}G(n,2)$, i.e., $\{0,x\}$ is a one-dimensional subspace of $\mathbb{F}^{n+1}$, then we denote x by $a_1\cdots a_s$ where $x = e_{a_1}+\cdots+e_{a_s}$ is the unique expansion of x in the given basis. For example, the element $x = e_0+e_2+e_3$ is denoted 023. We shall call elements of $\mathbb{P}G(n,2)$ *words* and we say that $a_1\cdots a_s$ is a word of *length s*

* Corresponding author. E-mail: wehlau@mast.queensu.ca.

[1] This research is partially supported by NSERC Grants.

0378-3758/97/$17.00
SSDI 0378-3758(96)00161-9

(with respect to the basis $\{0,\dots,n\}$). The structure of $\mathbb{F}^{n+1}$ as a vector space induces an analogous structure on $\mathbb{P}G(n,2)$. In particular, we can add elements of $\mathbb{P}G(n,2)$ by adding their representatives. The three points of $\mathbb{P}G(n,2)$ x, y and z form a *line* if $x+y=z$. Note that in this case we also have $x+z=y$ and $y+z=x$.

A subset X of $\mathbb{P}G(n,2)$ is called *independent* if it is line-free. Moreover, it is called *linearly independent* if it is linearly independent when considered as a subset of $\mathbb{F}^{n+1}$. For $2\leqslant k\leqslant n$, a subset $K\subseteq\mathbb{P}G(n,2)$ is a *k-flat* if $K\cup\{\vec{0}\}$ is a $(k+1)$-dimensional subspace of $\mathbb{F}^{n+1}$. Note that a k-flat is isomorphic to $\mathbb{P}G(k,2)$.

A *plane* is a 2-flat, a *hypersolid* is an $(n-2)$-flat and a *hyperplane* is an $(n-1)$-flat. The complement of a hyperplane is called an *affine subspace* of $\mathbb{P}G(n,2)$ and denoted by $\mathbb{A}G(n,2)$. Denote by $\mathscr{H}$ the set of all hyperplanes. Now it is well known that $K\in\mathscr{H}$ if and only if there is a $u_0\in\mathbb{P}G(n,2)$ such that

$$K=\{u_0\}^{\perp}:=\{\,v\in\mathbb{P}G(n,2): v\cdot u_0=0\,\},$$

where $\cdot$ represents the usual inner (or dot) product on $\mathbb{F}^{n+1}$.

A set C is said to be an *r-intersection-set* of $\mathbb{P}G(n,2)$ if $|C\cap K|\geqslant r$ for all $K\in\mathscr{H}$. Moreover, C is a *minimal r-intersection-set* if no proper subset of C is an r-intersection-set, i.e., every proper subset C' of C meets at least one hyperplane in less than r points. Moreover, a hyperplane $H\in\mathscr{H}$ is said to be *critical* for the r-intersection-set C (or briefly *critical*) if $|C\cap H|=r$. Note that C is a minimal r-intersection-set iff every element of C belongs to some critical hyperplane. Moreover, it is easy to see that every r-intersection-set A contains a minimal r-intersection-set C. Indeed, let $A_1:=A\backslash\{x_1\}$, where x_1 is a point of A (if any) that does not belong to any critical hyperplane. If A_1 is a minimal r-intersection-set, then we are done. Otherwise, we continue in this fashion to define the set C.

Let K_1 and K_2 be two hyperplanes. Then there are two elements x_1 and x_2 such that $K_i=\{x_i\}^{\perp}$, $i=1,2$. Then the hyperplane consisting of all elements orthogonal to x_1+x_2 is denoted by K_1+K_2, i.e., $K_1+K_2:=\{x_1+x_2\}^{\perp}$. Clearly, $\mathbb{P}G(n,2)=K_1\cup K_2\cup(K_1+K_2)$ and, moreover, $K_1\cap K_2=K_1\cap(K_1+K_2)=K_2\cap(K_1+K_2)$ is a hypersolid (i.e., is $\cong\mathbb{P}G(n-2,2)$).

2. Counting with polynomials

Let $C\subseteq\mathbb{P}G(n,2)$ and put $t:=|C|$. For $0\leqslant i\leqslant t$, define $n_i:=|\{K\in\mathscr{H}:|K\cap C|=i\}|$. The set $\{i:n_i\neq 0\}$ is called the *character of* C. Note that if C is a minimal r-intersection-set, then since every point of C lies in a critical hyperplane, we have $n_r\geqslant|C|/r$.

Consider the following equations (cf. Glynn, 1982):
Clearly,

$$\sum_i n_i=2^{n+1}-1,$$

and counting the number of pairs $\{p, K\}$ where $K \in \mathscr{H}$ and $p \in C \cap K$, we find

$$\sum_i in_i = (2^n - 1)t.$$

Now counting triples $\{p_1, p_2, K\}$ where $K \in \mathscr{H}$ and $\{p_1, p_2\} \subseteq C \cap K$ gives

$$\sum_i \binom{i}{2} n_i = (2^{n-1} - 1)\binom{t}{2}.$$

Moreover, suppose that the set C is independent, then by counting quadruples $\{p_1, p_2, p_3, K\}$ where $K \in \mathscr{H}$ and $\{p_1, p_2, p_3\} \subseteq C \cap K$ we obtain

$$\sum_i \binom{i}{3} n_i = (2^{n-2} - 1)\binom{t}{3}.$$

We remark that similar incidence equations may be easily written down for caps over any finite field.

Consider now a cubic polynomial $P(i) := (i - r_1)(i - r_2)(i - r_3)$. Write $a_3, \ldots, a_0$ such that $P(i) = a_3\binom{i}{3} + a_2\binom{i}{2} + a_1 i + a_0$ where the $a_i \in \mathbb{R}$. (Here $a_3 = 6$, $a_2 = -2(r_1 + r_2 + r_3) + 6$, $a_1 = r_1r_2 + r_1r_3 + r_2r_3 - (r_1 + r_2 + r_3) + 1$ and $a_0 = -r_1r_2r_3$.) Thus

$$\begin{aligned}\sum_i P(i)n_i &= a_3 \sum_i \binom{i}{3} n_i + a_2 \sum_i \binom{i}{2} n_i + a_1 \sum_i in_i + a_0 \sum_i n_i \\ &= a_3(2^{n-2} - 1)\binom{t}{3} + a_2(2^{n-1} - 1)\binom{t}{2} + a_1(2^n - 1)t + a_0(2^{n+1} - 1).\end{aligned}$$

This sum is a cubic polynomial of t, which is denoted $f_P(t)$. It turns out that $f_P(t)$ is quite useful for bounding t. For example, if we choose the roots r_1, r_2 and r_3 of $P(i)$ such that $P(i) \geqslant 0$ whenever $n_i \neq 0$, then $f_P(t)$ is nonnegative and this gives bounds on the values of t.

Example A. Suppose $C \subset \mathbb{P}G(5,2)$ is independent, has cardinality t and $|C \cap K| \geqslant 4$ for every $K \in \mathscr{H}$, i.e., $n_0 = n_1 = n_2 = n_3 = 0$. Consider the polynomial $P(i) := (i - 4)(i - 7)(i - 8)$. Clearly, $P(i) \geqslant 0$ for $i \geqslant 4$, and so $\sum_i n_i P(i) \geqslant 0$. But $f_P(t) = 7t^3 - 261t^2 + 3292t - 14\,112 \geqslant 0$ gives that $t \geqslant 13.6904, \ldots$, i.e., $t \geqslant 14$. This shows that any independent subset of $\mathbb{P}G(5,2)$ which meets every hyperplane $K \in \mathscr{H}$ in 4 points or more must contain at least 14 elements.

Example B. Let $C \subset \mathbb{P}G(5,2)$ be an independent set such that $|C \cap K| \geqslant 5$ for every $K \in \mathscr{H}$. Hence $n_0 = n_1 = n_2 = n_3 = n_4 = 0$. Consider the 7 polynomials $P_9(i), P_{10}(i), \ldots, P_{15}(i)$ defined by $P_9(i) := (i - 5)(i - 9)(i - 10)$, $P_{10}(i) := (i - 5)(i - 10)(i - 11), \ldots, P_{15}(i) := (i - 5)(i - 15)(i - 16)$. As $n_0 = n_1 = n_2 = n_3 = n_4 = 0$, we have that $\sum_i n_i P_j(i) \geqslant 0$ for all $j = 9, \ldots, 15$.

The bounds these seven polynomials give are summarized in Table 1

Table 1

Polynomial	Conditions on t
$P_9(i) = (i-5)(i-9)(i-10)$	$t \geqslant 19$
$P_{10}(i) = (i-5)(i-10)(i-11)$	$13 \leqslant t \leqslant 18$ or $t \geqslant 21$
$P_{11}(i) = (i-5)(i-11)(i-12)$	$12 \leqslant t \leqslant 21$ or $t \geqslant 24$
$P_{12}(i) = (i-5)(i-12)(i-13)$	$12 \leqslant t \leqslant 22$ or $t \geqslant 27$
$P_{13}(i) = (i-5)(i-13)(i-14)$	$12 \leqslant t \leqslant 24$ or $t \geqslant 29$
$P_{14}(i) = (i-5)(i-14)(i-15)$	$12 \leqslant t \leqslant 26$ or $t \geqslant 32$
$P_{15}(i) = (i-5)(i-15)(i-16)$	$12 \leqslant t \leqslant 28$ or $t \geqslant 35$

It is well-known that the size of the largest independent subset of $\mathbb{P}G(n,2)$ is 2^n and that every such set is an affine subspace. Thus every independent subset of $\mathbb{P}G(5,2)$ has cardinality at most 32, and the above table shows that $|C| = 21$. Now 21 is a root of both $f_{P_{10}}$ and of $f_{P_{11}}$. From $f_{P_{10}}(21) = 0$ we deduce that $n_i = 0$ for all values of i different from 5, 10 and 11. Similarly using $f_{P_{11}}(21) = 0$ shows that $n_i = 0$ for i different from 5, 11 and 12. Therefore if $n_i \neq 0$ then $i \in \{5, 11\}$. Now if we consider any two critical hyperplanes H_1 and H_2 we see that we must have $H_1 \cap H_2 \cap C = \emptyset$ (and $|(H_1 + H_2) \cap C| = 11$). Since no point lies in two critical hyperplanes we see that the critical hyperplanes must partition C and thus $|C| \equiv 0 \pmod 5$. This contradiction shows that there are no independent 5-intersection subsets of $\mathbb{P}G(5,2)$.

Example C. There are no independent 11-intersection subsets of $\mathbb{P}G(6,2)$. This can be shown in an entirely similar way using polynomials of the form $P_q(i) = (i-11)(i-q)(i-q-1)$ for $q = 17, 18, \ldots, 30$.

3. Intersection-sets

In this section, we shall construct a line-free 2^{n-3}-intersection-set in $\mathbb{P}G(n,2)$ for $n \geqslant 3$.

Let $n \geqslant 3$ and choose a hypersolid $I \subset \mathbb{P}G(n,2)$. There are three hyperplanes K_1, K_2 and $K_3 = K_1 + K_2$ which contain I. Choose another hypersolid $J \subset \mathbb{P}G(n,2)$ which is not contained in any of the K_i. Define $U_1 := K_1 \cap J$, $U_2 := K_2 \cap J$, $U_3 := K_3 \cap J$ and $U_3' := K_3 \backslash U_3$. Let $V_i := U_i \backslash I$ for $i = 1,2,3$ and $V_3' := (K_3 \backslash I) \backslash V_3$. Finally, we put $X_n := (V_1 \cup V_2 \cup V_3')$.

Note that $K_1 \cap X_n = V_1 \cong \mathbb{A}G(n-3,2)$ and $K_2 \cap X_n = V_2 \cong \mathbb{A}G(n-3,2)$. Also $K_3 \cap X_n = V_3' = (K_3 \backslash I) \backslash V_3$ where $K_3 \backslash I \cong \mathbb{A}G(n-1,2)$, $V_3 \subset (K_3 \backslash I)$ and $V_3 \cong \mathbb{A}G(n-3,2)$. Also it is easy to see that X_n is a maximal line-free subset of $\mathbb{P}G(n,2)$.

Lemma 1. *If $n \geqslant 3$ then $X_n \subset \mathbb{P}G(n,2)$ is a line-free 2^{n-3}-intersection-set of size $5(2^{n-3})$.*

Proof. First we show that X_n is line-free. Let $x_1, x_2 \in X_n$. If $x_1, x_2 \in K_i \cap X_n$ for some $i = 1, 2$ or 3 then $x_1 + x_2 \in I$ and thus $x_1 + x_2 \notin X_n$. If $x_1 \in V_1$ and $x_2 \in V_2$ then $x_1 + x_2 \in J \cap K_3$ and hence $x_1 + x_2 \notin X_n$, for the remaining case we may assume, by symmetry, that $x_1 \in V_1$ and $x_2 \in V_3'$. Then $x_1 + x_2 \in K_2 \backslash J$ and therefore $x_1 + x_2 \notin X_n$.

Now we show that X_n is a 2^{n-3}-intersection-set. First note that $|K_1 \cap X_n| = |K_2 \cap X_n| = |\mathbb{A}G(n-3,2)| = 2^{n-3}$. Also $|K_3 \cap X_n| = |\mathbb{A}G(n-1,2)| - |\mathbb{A}G(n-3,2)| = 2^{n-1} - 2^{n-3} = 3(2^{n-3})$. Let $H \in \mathscr{H}$ be any hyperplane other than K_1, K_2 and K_3. Then the hypersolid $H \cap K_3$ contains $2^{n-1} - 1$ points of which 2^{n-2} are not in I. Only 2^{n-3} points of $K_3 \backslash I$, are not contained in X_n and thus $|H \cap V_3'| \geq 2^{n-3}$. $\square$

For example, if $n = 3$ let $K_1 = \{012\}^{\perp}$, $K_2 = \{013\}^{\perp}$ and $K_3 = K_1 + K_2 = \{23\}^{\perp}$. Then $I = \{01, 123, 023\}$. Let $J = \{2, 3, 23\}$. Then $U_1 = \{3\}$, $U_2 = \{2\}$ and $U_3' = \{0, 1, 0123\}$. It is easy to check that every independent 1-intersection-set in $\mathbb{P}G(3,2)$ is isomorphic to $X_3 = \{0, 1, 2, 3, 0123\}$.

If $n = 4$, let $K_1 = \{0123\}^{\perp}$ and $K_2 = \{0124\}^{\perp}$. Then $K_3 = \{34\}^{\perp}$ and I is the plane generated by $\{01, 12, 234\}$. Take J to be the plane generated by $\{3, 4, 012\}$. Then $V_1 = \{4, 0123\}$, $V_2 = \{3, 0124\}$ and $V_3' = \{0, 1, 2, 0134, 0234, 1234\}$ and $X_4 = \{1, 2, 3, 4, 0123, 0124, 0134, 0234, 1234\}$.

Now we want to give another description of X_n. Let $v \in I \cap J$. Suppose $x \in V_i$. Then $x \in J \backslash I$. Let y be the third point on the line containing x and v. Then $y \in J \backslash I$. Since $x, y \in K_i$ it follows that $y \in V_i$. From this we also see that if $x' \in V_3'$ and $\{x', y', v\}$ is a line then $y' \in V_3'$. Hence we see that each line through v meets X_n in either 2 or 0 points. Now let H be any hyperplane not containing v. Let $Y = H \cap X_n$. Each line through v that contains a point of Y contains a further point of X_n not in H. Thus $|X_n| \geq 2|Y|$. On the other hand each line through v must intersect H and so $X_n| = 2|Y|$. We say that X_n is the *cone* on Y with *vertex* v. In fact, Y is the copy of X_{n-1}, constructed in H, with $I' = I \cap H$ and $J' = J \cap H$ playing the roles of I and J.

Therefore we have another, inductive, construction of X_n: Take a copy of $X_{n-1} \subset \mathbb{P}G(n-1,2) \subset \mathbb{P}G(n,2)$ and choose $v \in \mathbb{P}G(n,2) \backslash \mathbb{P}G(n-1,2)$. Then $X_n = \{y \mid \{x, y, v\}$ is a line and $x \in X_n\} \cup X_{n-1}$.

We can use this description to show that X_n is a *three character set* for $n \geq 4$. More precisely, if K is a hyperplane of $\mathbb{P}G(n,2)$ then $|X_n \cap K| \in \{2(2^{n-4}), 5(2^{n-4}), 6(2^{n-4})\}$. This is seen as follows. It is easy to check directly that $|X_3 \cap K| \in \{1, 3\}$. Now suppose that H is a hyperplane in $\mathbb{P}G(n,2)$ containing the vertex v described above. Then $H \cap \mathbb{P}G(n-1,2)$ is a hyperplane in $\mathbb{P}G(n-1,2)$ which meets X_{n-1} in k points (where $k \in \{2(2^{n-5}), 5(2^{n-5}), 6(2^{n-5})\}$). Then clearly X_n meets H in $2k$ points. On the other hand, if H is a hyperplane of $\mathbb{P}G(n,2)$ not containing v then H meets each line through v in exactly one point. Then, as above, $|H \cap X_n| = |X_{n-1}| = |X_n|/2$.

Next we show that every 2-intersection-set in $\mathbb{P}G(4,2)$ is isomorphic to X_4.

Lemma 2. *Let C be an independent subset of $\mathbb{P}G(4,2)$ of cardinality* 10. *Then either C is contained in an affine subspace of $\mathbb{P}G(4,2)$ or $C = \Phi(X_4)$ for some $\Phi \in \mathrm{Aut}(\mathbb{P}G(4,2))$.*

Proof. Suppose that C is not contained in an affine subspace of $\mathbb{P}G(4,2)$, hence C meets every hyperplane of $\mathbb{P}G(4,2)$; If C contains at most 4 linearly independent elements, then C is a subset of some copy of $\mathbb{P}G(3,2)$. But the largest independent subset of $\mathbb{P}G(3,2)$ has cardinality 8.

So let $0,1,2,3,4$ be a basis of $\mathbb{P}G(4,2)$ contained in C. As C contains no words of length two and $|C \cap \{01234\}^{\perp}| \geqslant 1$, we have that C contains at least one word of length four. Without loss of generality we may assume that this word is 0123. Thus $C \cap \{012, 013, 023, 123\} = \emptyset$. Now C can contain at most one element of each of the following three sets: $\{014, 234\}$, $\{024, 134\}$, and $\{124, 034\}$. Hence if C contains only the single word 0123 of length 4 then $|C| \leqslant 9$.

Suppose now C contains exactly two words of length 4. Again without loss of generality we may assume that these words are 0123 and 0124. Here the only words available to be added to C are 234, 134 and 034. Thus $C = \{0,1,2,3,4,0123,0124, 034,134,234\}$. Now the automorphism Φ of $\mathbb{P}G(4,2)$ defined by $\Phi(i) = i$ for $i \in \{0,1,2,4\}$ and $\Phi(3) = 0123$ satisfies $\Phi(C) = X_4$.

If C contains exactly three words of length four then it can contain at most one word of length three and thus $|C| \leqslant 9$. Finally, if C contains four or more words of length four then it can contain no words of length three. Thus, C contains all five words of length four and $C = X_4$. □

As the set X_4 is a maximal independent set in $\mathbb{P}G(4,2)$ we have the following:

Corollary 3. *If C is an independent set of $\mathbb{P}G(4,2)$ with $|C| \geqslant 11$, then C is contained in an affine subspace of $\mathbb{P}G(4,2)$.*

Next we consider $n = 5$. Let $C \subset \mathbb{P}G(5,2)$ be an independent 4-intersection-set. We first show that there is at least one hyperplane K such that $|C \cap K| \geqslant 12$. Then using this property we show that the C must be isomorphic to X_5.

Proceeding by contradiction we suppose that C is a minimal independent 4-intersection-set such that $n_i = 0$ for all $i \geqslant 12$. Put $t := |C|$.

Claim 4. $|C| \leqslant 19$.

Proof. Consider the polynomial $P(i) = (i-9)(i-10)(i-11)$. Then as $P(i) \leqslant 0$ for $i = 4, \ldots, 8$, we have that $\sum_{i=4}^{8} n_i P(i) \leqslant 0$, and so $f_P(t) = 7t^3 - 426t^2 + 8789t - 62\,370 \leqslant 0$. Hence $f_P(t) = n_4 P(4) + \sum_{i=5}^{8} n_i P(i) \leqslant 0$. Here $P(4) = -210$ and so $f_P(t) + 210 n_4 = \sum_{i=5}^{8} n_i P(i) \leqslant 0$. As C is minimal, $n_4 \geqslant \frac{1}{4}t$, and so $7t^3 - 426t^2 + 8789t + \frac{210}{4}t - 62\,370 \leqslant 0$, which implies that $t \leqslant 19$. □

Claim 5. $|C| \leqslant 17$.

Proof. From Claim 4 we have that $t \leqslant 19$. If for every pair of critical hyperplanes H_1 and H_2 we have that $(C \cap H_1) \cap (C \cap H_2) = \emptyset$, then $t = 4m$ for some positive integer m, and so $t \leqslant 16$. Suppose then that there are two critical hyperplanes H_1 and H_2 such that $a := |(C \cap H_1) \cap (C \cap H_2)| \geqslant 1$. Put $K := H_1 + H_2$. Then, as $C \subseteq C \cap (H_1 \cup H_2 \cup K)$, we have that $|C\cap K|\geqslant t-8+2a\geqslant t-6$. Therefore, if $t\geqslant 18$, we get that $|C\cap K|\geqslant 12$, a contradiction with $n_j=0$ for all $j\geqslant 12$. □

Claim 6. $n_{11}=0$.

Proof. Suppose that $n_{11}\neq 0$; hence there is a hyperplane $K\in\mathscr{H}$ such that $|C\cap K|=11$, and, therefore, $C\cap K$ is contained in an affine subspace of $\mathbb{P}G(4,2)$, i.e., there is a hypersolid $S\subseteq K$ such that $(C\cap K)\cap S=\emptyset$. Now the hypersolid S is contained in two more hyperplanes, K_1 and $K_2:=K+K_1$ with $S=K\cap K_1=K\cap K_2=K_1\cap K_2$. As $C\subseteq K\cup K_1\cup K_2$, we have that $|C|=|C\cap K|+|C\cap K_1|+|C\cap K_2|\geqslant 11+4+4=19$, contradicting Claim 5. □

Therefore, $n_j=0$, for all $j\geqslant 11$.

Claim 7. $|C|\geqslant 15$.

Proof. By Example A above, we have that $t\geqslant 14$. Suppose $t=14$ and consider the polynomial $P(i)=(i-4)(i-7)(i-8)$. Then $f_P(t)=7t^3-261t^2+3292t-14\,112$ and $f_P(14)=28$. As $P(10)=36$ and $P(9)=10$, we deduce that $n_{10}=0$ and $n_9\leqslant 2$. Let H_1 and H_2 be two distinct critical hyperplanes. As $|C\cap H_i|=4$, we have that $C\cap H_i$ is contained in some hypersolid S_i, $i=1,2$. Let H_i,K_i and L_i be the three hyperplanes that contain the hypersolid S_i, $i=1,2$, where $L_i=H_i+K_i$. Also $t=14$ implies that $|C\cap K_i|+|C\cap L_i|=18$. Combining this with $n_{10}=0$, we obtain that $|C\cap K_i|=|C\cap L_i|=9$, $i=1,2$. Now it is easy to see that $|\{K_1,L_1,K_2,L_2\}|\geqslant 3$. Indeed if $K_1=K_2$, then $L_1=K_1+H_1\neq K_1+H_2=L_2$, as $H_1\neq H_2$. Thus there are at least three distinct hyperplanes that meet C in 9 points, contradicting $n_9\leqslant 2$. □

We now collect all the results above to show the following:

Lemma 8. *If C is an independent 4-intersection-set of $\mathbb{P}G(5,2)$, then $|C\cap K|\geqslant 12$ for at least one $K\in\mathscr{H}$.*

Proof. Since every 4-intersection-set contains a minimal 4-intersection-set, it suffices to prove the result for C minimal. So let C be a minimal 4-intersection-set and take H a critical hyperplane for C. Let S be a hypersolid containing $C\cap H$. The hypersolid S is contained in three hyperplanes H,K_1 and K_2. Since $n_j=0$ for all $j\geqslant 11$, we have that $|(C\cap K_i)\backslash(C\cap H)|\leqslant 6$, for $i=1,2$. If $|(C\cap K_i))\backslash(C\cap H)|\leqslant 5$ for both $i=1,2$, then $|C|\leqslant 5+5+4=14$, which contradicts Claim 5. So suppose that $|(C\cap K_1)\backslash(C\cap H)|=6$, thus $|C\cap K_1|=10$ and we have two cases:

(i) $C\cap K_1$ is contained in an affine subspace of $\mathbb{P}G(4,2)$. Then as in the proof of Claim 6, we can show that $|C|\geqslant 18$, contradicting Claim 5.

(ii) $C\cap K_1\cong X_4$. Now as the character of X_4 is $\{2,5,6\}$, X_4 cannot meet a hyperplane of $\mathbb{P}G(4,2)$ (i.e., a hypersolid of $\mathbb{P}G(5,2)$) in exactly 4 points, but as $|C\cap S|=4$, this is a contradiction. □

We can now prove the following:

Theorem 9. *Up to isomorphism, X_5 is the unique independent 4-intersection-set in $\mathbb{P}G(5,2)$.*

Proof. We need to show that every independent 4-intersection-set in $\mathbb{P}G(5,2)$ is isomorphic to X_5. Consider an independent 4-intersection-set A of $\mathbb{P}G(5,2)$. Choose $C \subseteq A$, a minimal 4-intersection-set. By Lemma 8, $|C \cap K_3| \geqslant 12$ for some hyperplane $K_3 \in \mathscr{H}$. By Corollary 3, $C \cap K_3$ is contained in some affine subspace of $\mathbb{P}G(4,2)$, i.e., there is a hypersolid $I \subset K_3$ of $\mathbb{P}G(5,2)$ such that $C \cap I = \emptyset$. Now the hypersolid I is contained in three hyperplanes K_1, K_2 and K_3 of $\mathbb{P}G(5,2)$. As C is a 4-intersection-set, it meets each of K_1 and K_2 in at least 4 points. Since $I \subseteq K_i$, we have that $C \cap K_i \subseteq (K_i \backslash I)$, $i = 1,2$. Put $C_i := \{a_i, b_i, c_i, d_i\} \subseteq C \cap K_i$ and consider the sets $W_y := \{y+a_2, y+b_2, y+c_2, y+d_2\}$ for $y \in \{a_1, b_1, c_1, d_1\}$. Note that $W_y \subseteq K_3 \backslash I$. Since $|K_3 \backslash I| = 16$ and that $W_y \cap C = \emptyset$ we see that $|K_3 \cap C| = 12$ and $|K_2 \cap C| = 4$. Similarly, $|K_1 \cap C| = 4$ and thus $|C| = 20$. Also the four sets W_y for $y \in \{a_1, b_1, c_1, d_1\} = K_1 \cap C$ must coincide. In particular $W_{a_1} = W_{b_1}$. As $a_1 + a_2 \neq b_1 + a_2$, we may assume without loss of generality that $a_1 + a_2 = b_1 + b_2$ (1); hence $a_1 + b_2 = b_1 + a_2$. Moreover, this implies $a_1 + c_2 = b_1 + d_2$ (2) and $a_1 + d_2 = b_1 + c_2$. Adding Eqs. (1) and (2) gives $a_2 + c_2 = b_2 + d_2$. Thus, $a_2 = b_2 + c_2 + d_2$, which gives that $y + a_2 = (y+b_2) + (y+c_2) + (y+d_2)$, for all $y \in \{a_1, b_1, c_1, d_1\}$. Therefore, if we let J be the hypersolid of $\mathbb{P}G(5,2)$ generated by $\{a_1, b_1, c_1, a_2\}$ we find that C is the copy of X_5 constructed using J and I. Also, since X_5 is a maximal line-free set, $C = A$. □

Corollary 10. *If C is an independent subset of $\mathbb{P}G(5,2)$ with $|C| \geqslant 20$, then either C is contained in a affine subspace of $\mathbb{P}G(5,2)$ or $C = \Phi(X_5)$ for some $\Phi \in \mathrm{Aut}(\mathbb{P}G(5,2))$.*

Proof. Let C be an independent subset of $\mathbb{P}G(5,2)$ and suppose that C is not contained in some affine subspace of $\mathbb{P}G(5,2)$. Hence C is a 1-intersection set. Suppose moreover that C is not an automorphic image of X_5, hence $|C \cap K_0| \leqslant 3$ for some hyperplane $K_0 \in \mathscr{H}$. Put $m_0 := |C \cap K_0|$, and note that as C is a 1-intersection-set, $m_0 > 0$. Moreover it is clear that $C \cap S = \emptyset$ for some hypersolid $S \subseteq K_0$. Now the hypersolid S is contained in three hyperplanes K_0, K_1 and K_2, where $K_2 = K_0 + K_1$. As $|C| \geqslant 20$ and $C = (C \cap K_0) \cup (C \cap K_1) \cup (C \cap K_2)$, we have that $|C \cap K_i| \geqslant 9$ for at least one $i = 1,2$. So let $\{a_1, a_2, \ldots, a_s\} \subseteq C \cap K_1$ where $s \geqslant 9$. Let $a \in C \cap K_0$, then as C is independent, $C \cap \{a+a_1, \ldots, a+a_s\} = \emptyset$, where $\{a+a_1, \ldots, a+a_s\} \subseteq (K_2 \backslash S)$. Therefore, $|C \cap K_2| \leqslant 31 - (15 + s) = 16 - s$, and so $|C| \leqslant m_0 + s + (16 - s) \leqslant 19$, contradicting $|C| \geqslant 20$. This shows that if C is not contained in an affine subspace of $\mathbb{P}G(5,2)$, then it is a 4-intersection-set, and Theorem 9 completes the proof. □

Conjecture. Let $\tau(n)$ be the largest r for which there exists an independent r-intersection-set in $\mathbb{P}G(n,2)$. The set X_n shows that $\tau(n) \geqslant 2^{n-3}$ for $n \geqslant 3$. Here we have shown that $\tau(n) = 2^{n-3}$ for $n = 3,4$ and 5. We conjecture that $\tau(n) = 2^{n-3}$ for all $n \geqslant 3$ and that every independent 2^{n-3}-intersection-set is isomorphic to X_n.

References

Anderson, I. (1990). *Combinatorial Designs, Construction Methods*. Halsted Press, New York.

Bruen, A. (1992). Polynomial multiplicities over finite fields and intersection-sets. *J. Combin. Theory Ser. A* **60**, 19–32.

Fugère, J., L. Haddad and D. Wehlau (1994). 5-chromatic Steiner triple systems. *J. Combin. Designs* **2** (5), 287–299.

Glynn D.G. (1982). A lower bound for maximal partial spreads in $\mathbb{P}G(3,q)$. *Ars. Combin.* **13**, 39–40.

Pelikán, J. (1969). Properties of balanced incomplete block designs, In: *Combinat. Theory and its Applications*. Balatonfüred, Hungary. *Colloq. Math. Soc. János Bolyai* **4**, 869–889.