On characterizing designs by their codes

Bhaskar Bagchi[*]
Theoretical Statistics and Mathematics Division
Indian Statistical Institute
Bangalore - 560 059
India.

Abstract

We observe that the finite regular generalized polygons are characterized by their codes (over any field!): they are the only generalized polygons (with given parameters) which maximise the number of minimum weight words in the dual code. We conjecture that an analogous characterization (over $\mathbb{F}_p$, p the correct prime) holds at least for the point-line designs of a finite dimensional projective space over a prime field. In support of this conjecture, we present a weaker coding theoretic characterization of these designs in terms of the notion of "large clubs" introduced here. Along the way, we also prove a combinatorial characterization of the point-line designs of all finite projective spaces : apart from projective planes, these are the only Steiner 2-designs having as many hyperplanes as points.

A similar characterization of the desarguesian projective plane among projective planes of a prime order is not expected, except perhaps rather vacuously. However, we conjecture that the prime order desarguesian planes are characterized by maximising the number of words of the second minimum weight in their dual codes. We state a conjecture, on small linear spaces of prime order, whose validity is shown to imply this conjecture for projective planes.

[*]email: bbagchi@isibang.ac.in

1 Introduction

Use of coding theory in designs has a long history, by now.The monograph [1] is an excellent reference. Codes have been used to suggest constructions of designs (c.f. [7] for a nice example). They have also been used in non-existence results. A spectacular example is the proof of non-existence of projective planes of order ten (cf. [9]). Particularly in the presence of a moderately large group of automorphisms, codes can also be a powerful tool for characterization. For example, in [3] coding theory was used to prove that if a finite inversive plane of even order has a point-transitive automorphism group then it is a classical inversive plane. However, despite bright early promises coding theory has not yet been very successful in proving uniqueness results. The purpose of this paper is to suggest that, with a focus on the correct class of problems, this state of affairs can perhaps be improved upon substantially. Unfortunately, the results we present here are not as satisfactory as we had expected. But this is precisely what may attract younger researchers to the very attractive problems that we present here. We particularly wish to draw the attention of the reader to the "$3p - 3$ conjecture" in the last section.

Recall that an **incidence system** (finite throughout this article) is a triple (X, B, I) where X and B are finite sets (whose elements are called points and blocks, respectively) and $I \subseteq X \times B$ is a binary relation (called incidence) between points and blocks. The incidence system (X_0, B_0, I_0) is said to be a **sub-system** of the incidence system (X, B, I) if $X_0 \subseteq X$, $B_0 \subseteq B$ and $I_0 = I \cap (X_0 \times B_0)$. It is called an **induced subsystem** (or subsystem induced on X_0) if B_0 consists of all the blocks in B incident with at least one point in X_0.

It is customary to identify each block β of an incidence system with its shadow (i.e., the set of points incident with β). With this identification, the incidence relation becomes set inclusion $\in$. Although we shall ourselves occasionally fall in line with this custom (so that, for instance, we say that two blocks are disjoint if no point is incident with both), this has certain disadvantages : (a) sometimes blocks come with multiplicities, i.e., the "set" of blocks become a multi-set (and codes do not "see" this multiplicity), (b) the notion of sub-systems becomes some-what murky, (c) the obvious duality between points and blocks get lost, and (d) often, in a natural construction of an incidence system, the incidence relation is not set membership.

Given an incidence system $\mathcal{X} = (X, B, I)$ and a field $\mathbb{F}$, the $\mathbb{F}$-ary code $C_{\mathbb{F}}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the linear subspace of $\mathbb{F}^X$ generated by the "indicator" functions χ_β, $\beta \in B$. Here $\chi_B(x) = \begin{cases} 1 & \text{if } xI\beta \\ 0 & \text{otherwise} \end{cases}$. The $\mathbb{F}$-linear space $\mathbb{F}^X$ is equipped with a natural "inner product" (non-degenerate symmetric bilinear form) $\langle \cdot, \cdot \rangle$ defined by $\langle w_1, w_2 \rangle = \sum\limits_{x \in X} w_1(x)\ w_2(x)$, for $w_1, w_2 \in \mathbb{F}^X$. The dual $\mathbb{F}$-ary code $C_F^\perp(\mathcal{X})$ is defined to be the orthocomplement of its $\mathbb{F}$-ary code with respect to this inner product:

$$C_{\mathbb{F}}^\perp(\mathcal{X}) = \{w \in \mathbb{F}^X : \langle w, w' \rangle = 0 \ \forall \ w' \in C_{\mathbb{F}}(\mathcal{X})\}.$$

In particular, if $\mathbb{F} = \mathbb{F}_p$ is the finite field of prime order p, we write $C_p(\mathcal{X})$ and $C_p^\perp(\mathcal{X})$ for these two codes, and call them the **p-ary code** and the **dual p-ary code** of the incidence system $\mathcal{X}$. Clearly we have $dim\ C_p(\mathcal{X}) + dim\ C_p^\perp(\mathcal{X}) = \#(X)$.

More generally, a code is a linear subspace C of $\mathbb{F}^X$. We define its dual code $C^\perp$ exactly as above. For any "word" $w \in C$, its **support** is the point-set $\{x \in X : w(x) \neq 0\}$. The Hamming weight of w is the size of its support. The minimum of the weights of the non-zero words of a code is usually called the **minimum weight** of the code.

The following (admittedly some-what vague) principle is actually well known to experts, even though we are not aware of anybody ever writing it down explicitly.

The Fundamental principle of coding theory of designs:

The size of the dual p-ary code (for appropriate choice of the prime p) of a design (or incidence system) is a measure of the combinatorial regularity of the design. The larger the dual code, the more regular is the design.

This paper is an attempt to quantize this principle in various special cases. Actually, the original conjecture of Hamada and Sachar (briefly discussed in Section 3 below) is perhaps the first such attempt.

2 Generalized polygons

The **incidence graph** of an incidence system $\mathcal{X} = (X, B, I)$ is the graph with the disjoint union $X \sqcup B$ as vertex-set, such that $x \in X$ is adjacent with $\beta \in B$ iff $xI\beta$; and there are no other adjacencies. This incidence system is said to be a generalized polygon if (its incidence graph is connected and) the girth of its incidence graph is double its diameter. If the diameter is n then we talk of a generalized n-gon. For any finite generalized n-gon there are parameters s and t such that each block is incident with $s+1$ points and each point is incident with $t+1$ blocks. One talks of an (s,t)-generalized n-gon. It is called **thin** if $s = 1$ and **thick** otherwise. The ordinary polygons (i.e. cyclic graphs with vertices thought of as points, edges thought of as blocks) are the most obvious examples of generalized polygons (hence the name); they are thin. All other examples are called non-trivial. In this section, by "generalized polygon" we shall mean the non-trivial ones.

By a famous theorem of Feit and Higman (cf. [6]), all thick finite generalized polygons have $n = 3, 4, 6$ or 8. The generalized 3-gons (triangles) are just the projective planes. The following result is well known (and easy to prove):

Lemma 2.1 *Let $\mathcal{X}$ be a finite thin (non-trivial) generalized n-gon, say with parameter $(1,t)$. Then $\mathcal{X}$ is the incidence graph of a (t,t) generalized $\frac{n}{2}$-gon. Thus $n = 4, 6, 8$ or 12.*

(In the case $n = 4$, a generalized 2-gon is a trivial system in which each point is incident with each block. This is usually excluded from consideration - for instance in the statement of Feit-Higman theorem quoted above - since one implicitly assumes $n \geq 3$ in the definition of a generalized n-gon. Also, in the Lemma above, the case $n = 16$ is ruled out since there is no (t,t) generalized octagon.)

Definition 2.1 *Let $\mathcal{X}$ and $\mathcal{Y}$ be generalized n-gons (with the same n). We say that $\mathcal{Y}$ is a sub-generalized polygon of $\mathcal{X}$ if $\mathcal{Y}$ is a sub-system of $\mathcal{X}$. The thick generalized n-gon $\mathcal{X}$ with parameters (s,t) is said to be* **regular** *if any two points x, y of $\mathcal{X}$ at distance n (in the incidence graph) occur together in some (necessarily unique) sub-generalized n-gon with parameters $(1,t)$. (This definition is due to N.S.N. Sastry).*

The following result is actually a reformulation of an old theorem (Theorem 2.8 in [4]).

THEOREM 2.1 *(Bagchi and Sastry): Let $\mathcal{X}$ be a thick (s,t) - generalized n-gon, with $n = 2k$ even. (Thus $n = 4, 6$ or 8). Then, for any prime p, the minimum weight of $C_p^{\perp}(\mathcal{X})$ is at least $2(t^k - 1)/(t-1)$ and the dual code contains at most $\frac{p-1}{2}(s+1)(t-1)s^k((st)^k - 1)/(st-1)$ words of this weight. Further, equality holds in the last inequality (i.e., $\mathcal{X}$ maximises the number of minimum weight words in its dual code among all generalized polygons of the same parameter) for some prime p iff $\mathcal{X}$ is regular.*

Thus, if equality holds for some prime then it holds for all primes.

Proof: Usual counts show that the (s,t) generalized $2k$-gon $\mathcal{X}$ has exactly $(s+1)((st)^k - 1)/(st-1)$ points, and each point is at distance $n = 2k$ from exactly $s^k t^{k-1}$ points. Therefore there are
$M := (s+1)((st)^k - 1)s^k t^{k-1}/(st-1)$ ordered pairs of points at distance $2k$ in $\mathcal{X}$. Similarly, any $(1,t)$ sub-generalized $(2k)$-gon $\mathcal{Y}$ of $\mathcal{X}$ contains $N := 2t^{k-1}(t^k - 1)/(t-1)$ ordered pairs of points at distance $2k$. Now, it was shown in [4] that the minimum weight of $C_p^{\perp}(\mathcal{X})$ is at least $2(t^k - 1)/(t-1)$ and the support of a word of this weight must be the point sets of a $(1,t)$ sub-generalized $(2k)$-gon $\mathcal{Y}$ of $\mathcal{X}$. The argument there also shows that each pair of points at distance $2k$ in $\mathcal{X}$ are together in at most one such $\mathcal{Y}$. Therefore, there are at most $M/N = \frac{1}{2}(s+1)(t-1)s^k \cdot ((st)^k - 1)/(st-1)$ choices for $\mathcal{Y}$ (and hence for the support S of a minimum weight word). Clearly each such S supports exactly $(p-1)$ words of $C_p^{\perp}(\mathcal{X})$ (scalar multiples of each other). Hence the upper bound. Also, if S is the point set of a sub-generalized n-gon with parameter $(1,t)$, then by Lemma 2.1 we can write S as a disjoint union $S^+ \sqcup S^-$ where S^+ and S^- are the points and blocks of the associated (t,t) generalized k-gon. Then, any block of $\mathcal{X}$ is either non-incident with all points in S, or else it is incident with exactly one point from S^+ and exactly one point from S^-. Therefore the word w_S defined by

$$w_S(x) \begin{cases} 0 & \text{if} \quad x \notin S \\ 1 & \text{if} \quad x \in S^+ \\ -1 & \text{if} \quad x \in S^- \end{cases}$$

is in $C_p^{\perp}(\mathcal{X})$, and so are all its scalar multiples. Therefore, equality holds iff $\mathcal{X}$ is regular. □

Examples: The known regular generalized polygons are the following. (i) the "usual" (q,q) generalized quadrangle with automorphism group $Sp(4,q)$ (ii) the (q^2,q) generalized quadrangle with automorphism group $O(5,q)$ (iii) the "usual" (q,q) generalized hexagon with automorphism group $G_2(q)$, (iv) the (q^3,q) generalized hexagon with automorphism group ${}^3D_4(q)$ and (v) the (q^2,q) generalized octagon with automorphism group ${}^2F_4(q)$.

It is widely believed that these five series are actually characterized by regularity, and this is actually known in the case of the generalized quadrangles in (i) and (ii), cf. [12]. Thus Theorem 2.1 is a potential (actual for $n = 4$) coding theoretic characterization of these five series (among generalized polygons of the same parameters). This may be old wine in a new bottle, but it is our paradigm in the search for new coding theoretic characterizations. Notice, however, one peculiarity of generalized polygons revealed here which can not be expected of the 2-designs we study next :- Theorem 2.1 is characteristic free; its validity is independent of the choice of the prime p.

3 Dual codes of 2-designs

Recall that a $2-(v,k,\lambda)$ design (or 2-design with parameter v,k,λ) is an incidence system with v points such that each block is incident with k points (so k is called the block size) and any two distinct points are together incident with λ common blocks. One classical series of examples are the points versus t-flats incidence system $PG_t(n,\mathbb{F}_q)$ in the n-dimensional projective space $PG(n,\mathbb{F}_q)$ over the finite field $\mathbb{F}_q$ of order q. When $q = p^e$ with p prime (i.e., $p = \mathrm{char}(\mathbb{F}_q)$) the p-ary code (and its dual) of $PG_t(n,\mathbb{F}_q)$ seems to carry a huge amount of information about these designs. In [8] Hamada computed the dimensions of these codes.

Hamada (and independently Sachar) conjectured that $PG_t(n,\mathbb{F}_q)$ maximises the dimension of the dual p-ary code among all 2-designs with the same parameter. This conjecture is still open. However, they also made the stronger conjecture that $PG_t(n,\mathbb{F}_q)$ is actually characterised as the unique maximiser of the number of code words in the dual p-ary code. This stronger conjecture was refuted by Tonchev (cf. [13]) when he observed that there are exactly five distinct quasi-symmetric 2-(31,7,3) designs, including $PG_2(4,\mathbb{F}_2)$, and all of them have the same dimension 15 for their dual binary code. However, the strong conjecture may still be valid in some special cases, for instance for the points-versus-hyperplanes designs $PG_{n-1}(n, \mathbb{F}_q)$. In any case, this stronger conjecture is our model in the following discussions.

In [2] we proved a very general (and sometimes tight) lower bound on the minimum weight of the dual p-ary code of arbitrary incidence systems. This is our starting point. To state it, we need:

Definition 3.1 *Let $\mathcal{X}_i = (P_i, B_i, I_i)$, $i = 1, 2$, be two incidence systems and let λ be a positive integer. Then the λ-join of $\mathcal{X}_1$ and $\mathcal{X}_2$ is the incidence system $\mathcal{X}$ whose point-set is the disjoint union $P_1 \sqcup P_2$, and whose blocks are the blocks of $\mathcal{X}_1$ and $\mathcal{X}_2$ together with λ new blocks, say $(x_1, x_2)_i$, $1 \leq i \leq \lambda$, each incident with x_1 and x_2 and with no other points, for each $(x_1, x_2) \in P_1 \times P_2$.*

With this definition, the following is Theorem 2 from [2]:

Theorem 3.1 *(Bagchi and Inamdar): Let n, λ be positive integers and let p be a prime. Let $\mathcal{X}$ be any finite incidence system in which any two distinct points are together incident with at most λ blocks and each point is incident with at least $n + \lambda$ blocks. Then the minimum weight of the dual p-ary code $C_p^{\perp}(\mathcal{X})$ is at least $2(\frac{n}{\lambda} + 1 - \frac{n}{p\lambda})$. Further, a point-set S is the support of a word of $C_p^{\perp}(\mathcal{X})$ of this minimum weight if and only if the induced subsystem on S is the λ-join of two $2 - (\frac{n}{\lambda} + 1 - \frac{n}{\lambda p}, p, \lambda)$ designs.*

Notice that if $\mathcal{X}$ is any incidence system, say with point set P, then we may define $r(x)$ to be the number of blocks of $\mathcal{X}$ incident with x and $\lambda(x, y)$ to be the number of blocks of $\mathcal{X}$ incident with both x and y, for $x \neq y$ in P. Then, let's put $\lambda = \max\limits_{x \neq y} \lambda(x, y)$, $r = \min\limits_{x} r(x)$ and $n = r - \lambda$. Then Theorem 2 may be applied to $\mathcal{X}$ with this choice of n and λ, and any prime p. However, if we are looking for instances of equality in this theorem, then the parameters $(\frac{n}{\lambda} + 1 - \frac{n}{\lambda p}, p, \lambda)$ should satisfy the usual divisibility condition for a 2-design, in particular we must choose p to be a prime such that $p \mid n$.

Having said this, we are interested in investigating the cases of equality in Theorem 3.1 for 2-designs $\mathcal{X}$. Recall that if $\mathcal{X}$ is a $2 - (v, k, \lambda)$ design then each point of $\mathcal{X}$ is incident with r blocks, where the **replication number** r of $\mathcal{X}$ is given by $r(k-1) = \lambda(v-1)$. The number $n = r - \lambda$ is called the **order** of the 2-design, and it is known to play a key role in the coding theory of square designs. We introduce:

Definition 3.2 *A* **subdesign** *of a 2-design is a subsystem which is itself a 2-design. If D_1, D_2 are two subdesigns of a 2-design D then we say that D_1 and D_2 are* **totally disjoint** *if no point of D_1 is incident with any block of D_2 and no point of D_2 is incident with any block of D_1. (In particular, this implies that D_1 and D_2 have disjoint point-sets and disjoint block-sets. Notice that this definition would be very awkward to formulate if we identified blocks with subsets of the point-set!).*

In terms of this definition, the specialization of Theorem 3.1 to designs has the following interesting formulation. Unfortunately, the parameter λ of a $2-(v,k,\lambda)$ design has no standard name. In the following, we use the name **balance** for this parameter.

Theorem 3.2 *Let D be a 2-design of order n and balance λ. Then, for any prime p, the minimum weight of $C_p^{\perp}(D)$ is at least $2(\frac{n}{\lambda}+1-\frac{n}{\lambda p})$. Further, a set S of points of D is the support of a word of weight $2(\frac{n}{\lambda}+1-\frac{n}{\lambda p})$ in $C_p^{\perp}(D)$ if and only if S is the (disjoint) union of the point-sets of two totally disjoint $2-(\frac{n}{\lambda}+1-\frac{n}{p\lambda}, p, \lambda)$ subdesigns of D.*

Proof: The lower bound on minimum weight is from Theorem 3.1. Also if S is the support of a word of $C_p^{\perp}(D)$ attaining this bound, then by Theorem 3.1, S must be as stated. Conversely, let $S = S_1 \sqcup S_2$ where S_1, S_2 are the point-sets of totally disjoint subdesigns D_1, D_2 with the parameters given. Since D_i has the same balance λ as the design D, any block of D incident with two or more points of D_i must be a block of D_i (and hence incident with exactly p points of S_i and no point of S_j, $j \neq i$). Therefore, for any point $x \in S_1$, there are exactly $\lambda(\frac{n}{\lambda}+1-\frac{n}{p\lambda}) = n+\lambda-\frac{n}{p}$ blocks incident with x each of which is incident with a unique point in S_2. Since D_i has replication number $\frac{n}{p}$ and D has replication number $n+\lambda$, this shows that the induced subsystem of D on the point-set S is precisely the λ-join of D_1

and D_2. Therefore, by Theorem 3.1, S is the support of a word of $C_p^{\perp}(D)$. □

This has the following interesting consequence.

Corollary 3.1 *With notations as in Theorem 3.2, let $\mathcal{D}$ be the collection of all $2-(\frac{n}{\lambda}+1-\frac{n}{p\lambda}, p, \lambda)$ sub-designs of D. For $D_1, D_2 \in \mathcal{D}$ write $D_1 \sim D_2$ if either $D_1 = D_2$ or D_1 and D_2 are totally disjoint. Then $\sim$ is an equivalence relation on $\mathcal{D}$.*

Proof: Only transitively needs proof. So let D_1, D_2, D_3 be distinct members of $\mathcal{D}$ with $D_1 \sim D_2 \sim D_3$. Let P_i be the point-set of $D_i, 1 \leq i \leq 3$, and let P be the point-set of D. For $1 \leq i \leq 3$, let $w_i : P \to \mathbb{F}_p$ be the indicator function of P_i. Then by Theorem 3.2, $w_1 - w_2$ and $w_2 - w_3$ are words in $C_p^{\perp}(D)$. Therefore, their sum $w_1 - w_3$ is also in $C_p^{\perp}(D)$. Hence by Theorem 3.2, $D_1 \sim D_3$. □

Definition 3.3 *A* **club** *in a 2-design D of order n and balance λ is a maximal collection of pairwise totally disjoint $2-(\frac{n}{\lambda}+1-\frac{n}{\lambda p}, p, \lambda)$ subdesigns of D. In other words, it is an equivalence class of the relation $\sim$ in Corollary 3.1. (More precisely, this ought to be called a p-club, but the prime p will be clear from the context.)*

Notice that if S is the support of a minimum weight word in a p-ary code C then there are exactly $p-1$ words of C with support S; they are scalar multiples of each other. This is because if $w_1 \neq w_2$ are any two words with support S, then we can always choose a $\lambda \in \mathbb{F}_p^*$ such that the support of $w_2 - \lambda w_1 \in C$ is properly contained in S and hence $w_2 - \lambda w_1 = 0$. In view of this comment, the following is an obvious consequence of what we have seen so far:

Proposition 3.1 *If the 2-design D has t clubs, say of size $c_1, c_2, \ldots, c_t$, then the number of minimum weight words in $C_p^{\perp}(D)$ is $(p-1)\sum\limits_{i=1}^{t}\left(\begin{array}{c} c_i \\ 2 \end{array}\right)$.*

4 Codes of finite projective spaces

We specialize to the point-line designs $PG_1(n, \mathbb{F}_q)$. Notice that these are Steiner designs, i.e. they have balance $\lambda = 1$. We follow an usual convention and call all the blocks of Steiner 2-designs "**lines**". Although we shall soon specialize further to the case $q = p$, we begin with a purely combinatorial characterization of $PG_1(n, \mathbb{F}_q)$, q a power of the prime p. From now on, we identify lines of Steiner 2-designs with their shadows.

DEFINITION 4.1 *Let D be a Steiner 2-design. A* **flat** *F in D is a set of points such that F contains the line joining each pair of distinct points in F. It is a proper flat if F is a proper subset of the point-set of D. A* **hyperplane** *in D is a proper flat which meets every line of D.*

LEMMA 4.1 *The size of any proper flat F in a Steiner 2-design D is at most r, the replication number of D. Equality holds here iff F is a hyperplane of D.*

Proof: Fix a point x outside F. For any point y in F, let xy be the unique line joining x to y. Then $y \mapsto xy$ is a one-one function from F into the set of r lines through x. Hence $\#(F) \leq r$. Clearly equality holds in this argument iff F is a hyperplane. □

A 2-design is called trivial if each point is incident with each block; it is non-trivial otherwise. The parameters of any non-trivial 2-design satisfy Fisher's inequality $r \geq k$, equivalently $b \geq v$. Any 2-design satisfying equality here is called a **square** (or symmetric) design. A $2-(v, k, \lambda)$ design D is a square design iff its parameter satisfy $k(k-1) = \lambda(v-1)$. This holds iff the dual incidence system D^* is also a 2-design (necessarily with the same parameters as D) iff any two distinct blocks of D are together incident with exactly λ points. We also recall:

DEFINITION 4.2 *A* **line** *in a $2-(v, k, \lambda)$ design is a set of at least two points which is the intersection of λ distinct blocks. Clearly any two distinct points are together in a unique line. However, the lines of a 2-design need not form the lines of a Steiner 2-design since in general they may have variable sizes.*

Notice that the point-hyperplane design $PG_{n-1}(n, \mathbb{F}_q)$ is self dual; the lines of this square design are precisely the lines of $PG(n, \mathbb{F}_q)$. With this background, we have the following characterization of $PG_{n-1}(n, \mathbb{F}_q)$.

THEOREM 4.1 *(Dembowski and Wagner, cf. [10]): Let D be a square 2-design in which every line meets every block. Then either D is a projective plane (i.e. a square Steiner 2-design) or $D = PG_{n-1}(n, \mathbb{F}_q)$ for some $n \geq 3$ and prime power q.*

Now we state and prove a similar characterization of the point-line designs $PG_1(n, \mathbb{F}_q)$. Its proof is crucially dependent on the Dembowski-Wagner theorem.

THEOREM 4.2 *Let D be a Steiner 2-design on v points. Then D has at most v hyperplanes. Equality holds here iff either D is a projective plane or $D = PG_1(n, \mathbb{F}_q)$ for some $n \geq 3$ and some prime-power q.*

Proof: Let r and k be the replication number and block-size of D. Suppose D has v distinct hyperplanes; we must show that it has no more. Let $\mathcal{H}$ be a collection of v hyperplanes of D and let E be the incidence system with the point-set of D and with $\mathcal{H}$ as its set of blocks, incidence being set-membership. By Lemma 4.1, E has constant block size r. Also, any $H \in \mathcal{H}$ carries a $2-(r, k, 1)$ subdesign D_H of D, with replication number $= \frac{r-1}{k-1}$. If $H' \neq H$ is another number of $\mathcal{H}$, then $H' \cap H$ is a flat of D_H, and hence by Lemma 4.1, $\#(H' \cap H) \leq \frac{r-1}{k-1}$. Thus, each block of E has size r and any two distinct blocks of E have at most $\frac{r-1}{k-1}$ points in common. Therefore letting e_i denote the number of points which are in exactly i blocks of E, an obvious two-way counting yields :

$$\sum_{i \geq 0} e_i = v,$$

$$\sum_{i \geq 0} i\ e_i = rv,$$

$$\sum_{i \geq 0} i(i-1)e_i \leq v(v-1) \cdot \frac{r-1}{k-1} = r(r-1)v.$$

Therefore we get:

$$\begin{aligned} 0 &\leq \sum_{i\geq 0} (i-r)^2 e_i = \sum_{i\geq 0} i(i-1)e_i - (2r-1)\sum_{i\geq 0} i\ e_i + r^2 \sum_{i\geq 0} e_i \\ &\leq r(r-1)v - (2r-1)rv + r^2 v = 0. \end{aligned}$$

Therefore $\sum (i-r)^2 e_i = 0$. Thus $e_i = 0$ for $i \neq r$. This means that each point of E is in exactly r blocks of E. Also the inequalities in the above argument must actually be equalities. Thus any two distinct blocks of E have exactly $\frac{r-1}{k-1}$ points in common. This means that the dual E^* of E is a $2-(v, r, \frac{r-1}{k-1})$ design. Since this design has $b = v$, it is square. Therefore E itself is a square design. Now notice that any block of a design is uniquely determined by its remaining blocks (the incidence system consisting of the remaining blocks has two replication numbers $r-1$ and r, and the missing block must consist of the points of replication $r-1$). However, if there is a hyperplane H of D outside $\mathcal{H}$, then replacing any particular block of E by the new block H one obtains another 2-design (by the above argument), contrary to the observation just made.

Thus if D has at least v hyperplanes then it has exactly v hyperplanes (proving the inequality) and in that case the hyperplanes of D form the blocks of a square design E. From the definition of hyperplane one sees that every line of E contains a (unique) line of D and every line of D meets every block of E. Therefore every line of E meets every block of E. Therefore, by Theorem 4.1, E is either a projective plane (in which case $D = E$ is a projective plane) or else $E = PG_{n-1}(n, \mathbb{F}_q)$. In the latter case, comparing parameters of D and E, one sees that the lines of D are precisely the lines of $PG_{n-1}(n, \mathbb{F}_q)$, so that $D = PG_1(n, \mathbb{F}_q)$. □

Now we specialize further to the case $q = p$. Let D be a $2-(\frac{p^{n+1}-1}{p-1}, p+1, 1)$ design, p prime. By Definition 3.3, a club in D is a maximal collection of pairwise totally disjoint $2-(p^{n-1}, p, 1)$ subdesigns of D. Therefore, letting $v = \frac{p^{n+1}-1}{p-1}$. $v_0 = p^{n-1}$, we see that any club in D has at most $\lfloor \frac{v}{v_0} \rfloor = p+1$ members. This leads to :

Definition 4.3 *A* **large club** *in a* $2-(\frac{p^{n+1}-1}{p-1}, p+1, 1)$ *design is a club with* $p+1$ *members.*

Then we have :

Theorem 4.3 *For a prime p, any $2-(\frac{p^{n+1}-1}{p-1}, p+1, 1)$ design D has at most as many large clubs as there are lines of D. If $n \geq 3$, equality holds here iff $D = PG_1(n, \mathbb{F}_p)$.*

Proof: Let $D_0, D_1, \ldots, D_p$ be a large club, with corresponding point sets $P_0, P_1, \ldots, P_p$. Let P be the point set of D and put $Q = P \backslash (P_0 \sqcup \ldots \sqcup P_p)$. By Theorem 3.2, for $i \neq j$, the subsystem induced by D on $P_i \sqcup P_j$ is the join (i.e. 1-join) of D_i and D_j. It follows that for $0 \leq i \leq p$, $H_i = Q \sqcup P_i$ is a hyperplane of D and Q is a flat of size $\frac{p^{n-1}-1}{p-1}$. We call a flat of this size a **coline** of D. Thus, with any large club in D we have associated a coline Q which is contained in $p+1$ hyperplanes.

Now notice that if Q is a coline and $x \notin Q$ a point, then there is at most one hyperplane $H \supseteq Q \cup \{x\}$. H must be the union of the lines joining x to the points of Q. Thus the hyperplanes through Q are pairwise disjoint outside Q. Hence any coline is in at most $p+1$ hyperplanes, and equality holds when it is associated with a large club. It follows that any coline is associated with at most one large club. The members D_i of a large club associated with the coline Q must be the subdesigns of D carried by $H_i \backslash Q$, where H_i are the hyperplanes through Q. Thus the map from large clubs to colines is injective.

Now suppose D has (at least) b large clubs, where b is the number of lines of D. Thus D has b colines each of which is the intersection of $\binom{p+1}{2}$ pairs of hyperplanes. Thus there are (at least) $\binom{p+1}{2}b$ unordered pairs of hyperplanes in D. Letting N denotes the total number of hyperplanes in D, we deduce that $\binom{N}{2} \geq \binom{p+1}{2}b = \binom{v}{2}$, where v is the number of points of D. Therefore $N \geq v$. Hence by Theorem 4.2, $N = v$ and (if $n \geq 3$) $D = PG_1(n, \mathbb{F}_p)$. $\square$

Notice that the proof of Theorem 4.3 (applied to $D = PG_1(n, \mathbb{F}_p)$) shows that $C_p^{\perp}(PG_1(n, \mathbb{F}_p))$ has minimum weight $2p^{n-1}$ and its words of minimum weight are precisely the non-zero scalar multiples of the words $w_1 - w_2$ where w_1, w_2 are indicator functions of distinct hyperplanes of $PG(n, \mathbb{F}_p)$. This is actually a special case of Proposition 2 in [2].

Theorem 4.3 is actually a characterization of $PG_1(n, \mathbb{F}_p)$, $n \geq 3$, by its dual p-ary code, even if this is somewhat obscured by the technical terms. But we would like to prove:

Conjecture 4.1 *Let D be a $2-(\frac{p^{n+1}-1}{p-1}, p+1, 1)$ design, $n \geq 3$, p prime. Then $C_p^{\perp}(D)$ has at most $\frac{p}{2}(p^n-1)(p^{n+1}-1)/(p-1)$ words of (minimum) weight $2p^{n-1}$. Equality holds here iff $D = PG_1(n, \mathbb{F}_p)$.*

In view of Theorem 4.3, it suffices to show that if D has the right number of totally disjoint pairs of $2-(p^{n-1}, p, 1)$ subdesigns, then there must be the right number of large clubs.

5 Projective planes of prime order

We recall that a projective plane is just a square Steiner 2-design. Thus a projective plane of order n is nothing but a $2-(n^2+n+1, n+1, 1)$ design. It is a folklore conjecture that, for each prime p, there is a unique projective plane of order p, namely the desarguesian plane $PG_1(2, \mathbb{F}_p)$. Indeed, since the dual p-ary code of any projective plane of order p is easily seen to have dimension $\binom{p+1}{2}$, this conjecture may be seen as a special case of the strong Hamada-Sachar conjecture.

Thus it is specially interesting to obtain coding theoretic characterizations of $PG_1(2, \mathbb{F}_p)$. Such a characterization will provide a powerful tool to attack the uniqueness conjecture.

Theorem 3.2 from Section 3 specializes to the following result, first proved by Inamdar.

Corollary 5.1 *Let π be a projective plane of prime order p. Then the minimum weight of $C_p^{\perp}(\pi)$ is $= 2p$ and, up to multiplication by non-zero scalars, the words of minimum weight in $C_p^{\perp}(\pi)$ are $w_1 - w_2$, where w_1, w_2 are indicator functions of distinct lines.*

Since this holds for all putative projective planes of order p, the minimum weight words of the dual code fail to distinguish them. We suspect that looking at the second minimum weight will suffice. But what is the second minimum weight for the dual p-ary code even for the desarguesian plane $PG_1(2, \mathbb{F}_p)$? Nobody knows! In [5] it was shown that this weight is at least

$\frac{5}{2}(p+1)$ for $p \geq 11$. The following result shows that this weight is at most $3p-3$ for every prime $p \geq 5$. Note that when $p = 11$, the upper and lower bounds coincide, so that the second minimum weight is $3p-3$ in this case. Indeed, calculations show that it is $3p-3$ for $5 \leq p \leq 11$.

THEOREM 5.1 *For any prime $p \geq 5$, the dual p-ary code of $PG_1(2, \mathbb{F}_p)$ contains at least $\frac{1}{6}\ p^3(p^3-1)(p^2-1)$ words of weight $3p-3$.*

Proof: Take a point x, three distinct lines ℓ_1, ℓ_2, ℓ_3 through x and a line ℓ not passing through x. Put $S = (\ell_1 \cup \ell_2 \cup \ell_3) \backslash (\ell \cup \{x\})$. Thus S is a set of size $3p-3$. It is enough to construct one word of $C_p^{\perp}$ with support S. To this end, we set up co-ordinates such that ℓ is the line at infinity, x is the origin, and ℓ_1, ℓ_2, ℓ_3 are the lines with equation $Y = 0, X = 0$ and $Y = X$. Notice that, in this co-ordinate system, S consists of $3p-3$ affine points. Define the word w by setting $w(P) = 0$ for any point P of the projective plane, $P \notin S$, and define it on S by the formula

$$w(\alpha, \beta) = \begin{cases} 1/\alpha & \text{if } \ \beta = 0, \alpha \neq 0 \\ 1/\beta & \text{if } \ \alpha = 0, \beta \neq 0 \\ -1/\alpha & \text{if } \ \alpha = \beta \neq 0. \end{cases}$$

Then it is easy to see that w is a word of $C_p^{\perp}$, with support S. Therefore S supports (at least, but one can show exactly) $p-1$ words of $C_p^{\perp}$, namely the non-zero scalar multiples of w. Since there are $(p^2+p+1) \times p^2 \times \binom{p+1}{3}$ choices for S, we are done. □

Notice that in Theorem 5.1, p could be any prime power. But, when p is not prime, the words obtained are defined only over $\mathbb{F}_p$ and not over its prime subfield. In view of the comments preceding Theorem 5.1, we suspect that when p is prime, the second minimum weight of $C_p^{\perp}(PG_1(2, \mathbb{F}_p))$ is $3p-3$ and the words described in that theorem are its only words of weight $3p-3$. But we go ahead and state a much stronger conjecture (a priori stronger, that is!).

We recall that a **linear space** is an incidence system with exactly one line joining any two distinct points, and each line containing at least two points. We shall say that a linear space is of **order** p if each of its points is in exactly

$p+1$ lines. Clearly any linear space of order p has at most p^2+p+1 points, with equality only for projective planes of order p. Thus, there are only finitely many linear spaces of any given order, and the projective planes are the largest among them.

Definition 5.1 *An incidence system $\mathcal{X}$ is said to be non-trivial at a prime p if $C_p^{\perp}(\mathcal{X}) \neq \{0\}$.*

Examples of small linear spaces of order p which are non-trivial at the prime p:

(a) Let $\mathcal{X}_p$ be the linear space with two disjoint "long lines" ℓ_1, ℓ_2 of size p each and p^2 short lines of size two each joining a point of ℓ_1 to a point of ℓ_2. The word sending each point of ℓ_1 to $+1$ and each point of ℓ_2 to -1 is in $C_p^{\perp}(\mathcal{X}_p)$. Thus $\mathcal{X}_p$ is non-trivial at p.

(b) For $p \geq 3$, let $\mathcal{Y}_p$ be the linear space on $3p-3$ points described as follows. Its point-set is $\mathbb{F}_p^* \times \{1,2,3\}$. It has three long lines $\ell_i = \mathbb{F}_p^* \times \{i\}$, $i = 1,2,3$, of size $p-1$ each. It has $(p-1)(p-2)$ lines of size 3, namely $\{(\alpha_1,1),(\alpha_2,2),(\alpha_3,3)\}$ where $\alpha_1,\alpha_2,\alpha_3 \in \mathbb{F}_p^*$ with $\alpha_1+\alpha_2+\alpha_3 = 0$. It also has $3p-3$ lines of size 2, namely $\{(\alpha_1,i),(\alpha_2,j)\}$ where $1 \leq i \neq j \leq 3$, $\alpha_1,\alpha_2 \in \mathbb{F}_p^*$ with $\alpha_1+\alpha_2 = 0$. It is easy to verify that $\mathcal{Y}_p$ is a linear space of order p. The word $w : (\alpha, i) \mapsto \alpha$ is clearly a non-trivial word in $C_p^{\perp}(\mathcal{Y}_p)$. Thus $\mathcal{Y}_p$ is non-trivial at p.

Inamdar deduced Corollary 5.1 from the following result by looking at the subsystem of π induced on the support of a minimum weight word in $C_p^{\perp}(\pi)$:

Proposition 5.1 *: For primes p, $\mathcal{X}_p$ is the unique smallest linear space of order p which is non-trivial at p. That is, it has the smallest number $(2p)$ of points among all such spaces.*

Proof: This is the special case $n = p, \lambda = 1$ of Theorem 3.1. □

Conjecture 5.1 *(The $3p-3$ conjecture): For primes $p \geq 5$, $\mathcal{Y}_p$ is the unique second smallest linear space of order p which is non-trivial at p.*

That is, we conjecture that if Z is a linear space of prime order $p \geq 5$ which is non-trivial at p, then either $Z = \mathcal{X}_p$ or $Z = \mathcal{Y}_p$ or Z has at least $3p-2$ points.

Clearly $\mathcal{X}_p$ is obtained as the induced subsystem of $PG_1(2, \mathbb{F}_p)$ on the support of a minimum weight word of its dual code, and $\mathcal{Y}_p$ is obtained as the induced subsystem on one of the words described in Theorem 5.1. This is why they are non-trivial at p. Indeed, in our final result, we shall show that Conjecture 5.1 implies the following coding theoretic characterization of $PG_1(2, \mathbb{F}_p)$ among projective planes of order p:

Conjecture 5.2 *Let π be a projective plane of prime order $p \geq 5$. Then the second minimum weight of $C_p^{\perp}(\pi)$ is $\geq 3p-3$ and there are at most $\frac{1}{6}\, p^3(p^3-1)(p^2-1)$ words of weight $3p-3$ in this code. If, further, both π and its dual π^* satisfy equality in the last inequality then $\pi = PG_1(2, \mathbb{F}_p)$.*

Theorem 5.2 : *Conjecture 5.1 implies Conjecture 5.2.*

Proof: The first statement follows by looking at the induced subsystem of π on the support of words of weight $\leq 3p-3$. In view of the uniqueness statement in Conjecture 5.1, it also follows that the support S of any word in $C_p^{\perp}(\pi)$ of weight $3p-3$ is as described in the proof of Theorem 5.1. Hence the upper bound on the number of weight $3p-3$ words follows since the bound is just $(p-1)$ times the number of such sets S in π. If equality holds for π, then the induced subsystem on each such set S is isomorphic to $\mathcal{Y}_p$. This has the following translation. If $S = (\ell_1 \cup \ell_2 \cup \ell_3) \backslash (\ell \cup x)$ then, letting σ denote the affine plane obtained from π^* by deleting its "line" x, the Bruck subnet of σ corresponding to the three "points" ℓ_1, ℓ_2, ℓ_3 at infinity is co-ordinatized by the cyclic group of order p. Indeed, any word of $C_p^{\perp}(\pi)$ with support S provides such a co-ordinatization. As this holds for any three concurrent lines ℓ_1, ℓ_2, ℓ_3 of π, and since π^* is also assumed to satisfy the same, standard arguments imply that π must be desarguesian (cf. Proof of Theorem 5.1 in [11]). □

References

[1] E.F. Assmus and J.D. Key, *Designs and their codes*, Cambridge Tracts in Math. **103**, Cambridge Univ. Press, Cambridge, 1992.

[2] B. Bagchi and S.P. Inamdar, *Projective geometric codes*, J. Combin. Theory Series A **99** (2002), 128-142.

[3] B. Bagchi and N.S.N. Sastry, *Even order inversive planes, generalized quadrangles and codes*, Geom. Dedicata **22** (1987), 137-147.

[4] B. Bagchi and N.S.N. Sastry, *Codes associated with generalized polygons*, Geom. Dedicata **27** (1988), 1-8.

[5] V. Fack, S.L. Fancsali, L. Storme, G. Van de Voorde and J. Winne, *Small weight codewords in the codes arising from Desarguesian projective planes*, Designs, Codes and Cryptog. **46** (2008), 25-44.

[6] W. Feit and G. Higman, *The non-existence of certain generalized polygons*, J. Algebra **1** (1964), 114-131.

[7] M. Hall, jr., Combinatorial Theory, Second edition, Wiley publishers, New York, 1986.

[8] N. Hamada, *The rank of the incidence matrix of points and d-flats in finite geometries*, J. Sci. Hiroshima Univ., Ser. A1, **32** (1968), 381-396.

[9] C.W.H. Lam, L.H. Thiel and S. Swiercz, *The non-existence of finite projective planes of order 10*, Canad. J. Math. **41** (1989), 1117-1123.

[10] E.S. Lander, Symmetric designs: an algebraic approach, Cambridge Univ. Press, Cambridge, 1983.

[11] G.E. Moorhouse, *Bruck nets, codes and characters of loops*, Designs, Codes and Cryptog. **1** (1991), 7-29.

[12] S.E. Payne and J.A. Thas, Finite generalized quadrangles, Pitman advanced publishing program, London, 1984.

[13] V.D. Tonchev, *Quasi-symmetric 2-(31,7,7) designs and a revision of Hamada's conjecture*, J. Combin. Theory Ser. A, **42** (1986), 104-110.