The minimum weight of dual codes from projective planes

J. D. Key

Department of Mathematical Sciences
Clemson University, University of Wales Aberystwyth, University of the Western Cape and University of KwaZulu-Natal

October 19, 2007

Abstract

The minimum weight and the nature of the minimum-weight vectors of the p-ary codes from projective planes of order divisible by p was established in the 1960s, at an early stage of the study of these codes. The same cannot be said for the duals of these codes, where, in general, neither the minimum weight nor the nature of the minimum-weight words is known.

This talk will provide a survey of what is known of this problem, what progress has been made recently, and give some new bounds for planes of some specific orders.

Coding theory terminology

- A **linear code** is a subspace of a finite-dimensional vector space over a finite field.
- The **weight** of a vector is the number of non-zero coordinate entries. If a code has smallest non-zero weight d then the code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors by nearest-neighbour decoding.
- If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $\boldsymbol{[n, k, d]_q}$ to show this information.
- A **generator matrix** for the code is a $k \times n$ matrix made up of a basis for C.

Coding theory terminology continued

- The **dual** code $C^{\perp}$ is the orthogonal under the standard inner product $(,)$, i.e. $C^{\perp} = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$.
- A **check** matrix for C is a generator matrix H for $C^{\perp}$.
- Two linear codes of the same length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.
- An **automorphism** of a code C is an isomorphism from C to C.
- If C is the row span over any finite field of an incidence matrix for a plane then every automorphism (bijection that preserves points, lines and incidence) of the plane will give an automorphism of C, i.e.

$$\mathrm{Aut}(\mathbf{\Pi}) \subseteq \mathrm{Aut}(\boldsymbol{C}).$$

Definition

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, with point set $\mathcal{P} \neq \emptyset$, line set $\mathcal{L} \neq \emptyset$, $\mathcal{P} \cap \mathcal{L} = \emptyset$, and incidence $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$, is a projective plane if

- every set of two points are together incident with exactly one line;
- every set of two lines are together incident with exactly one point
- there are four points no three of which are collinear.

If $\mathcal{P}$ or $\mathcal{L}$ are finite, then there is an integer $n \geq 2$ such that

$$|\mathcal{P}| = |\mathcal{L}| = \boldsymbol{n^2 + n + 1}$$

and every line (point) is incident with exactly $\boldsymbol{n + 1}$ points (lines). $\boldsymbol{n}$ is the order of the plane.

All known planes have prime-power order and for every prime-power q there is at least one plane of this order, *viz.* the points and lines in projective 2-space over $\mathbb{F}_q$, $PG_2(\mathbb{F}_q)$.

Definition

The code $C_F(\Pi)$ or $C_q(\Pi)$ of a plane Π over the finite field $F = \mathbb{F}_q$ of order q is the space spanned by the incidence vectors of the lines over F, i.e. the row span over F of an incidence matrix with rows indexed by the lines, columns by the points.

Definition

The code $C_F(\Pi)$ or $C_q(\Pi)$ of a plane Π over the finite field $F = \mathbb{F}_q$ of order q is the space spanned by the incidence vectors of the lines over F, i.e. the row span over F of an incidence matrix with rows indexed by the lines, columns by the points.

If the plane has order n then only fields of characteristic prime p dividing n will give codes in this way that are of any interest, i.e. non-trivial (as codes). In fact only prime fields are needed.

Codes from planes

Some old results from the folklore, taken from [AK92]:

Theorem

Let Π be a projective plane of order n and let p be a prime dividing n.

- *The minimum-weight vectors of $C_p(\Pi)$, are precisely the scalar multiples of the incidence vectors of the lines, i.e. av^L, where $a \in \mathbb{F}_p$, $a \neq 0$, and L is a line of Π.*
- *The minimum weight of $C_p(\Pi)^\perp$ is at least $n+2$.*
- *If the minimum weight is $n+2$ then, $p=2$, n is even, and the minimum-weight vectors are all of the form v^X where X is a hyperoval of Π.*

Theorem

Let π be an affine plane of order n and p a prime dividing n.

- *Then the minimum weight of $C_p(\pi)$ is n and all minimum-weight vectors are constant.*
- *If $n = p$ the minimum-weight vectors of $C_p(\pi)$ are precisely the scalar multiples of the incidence vectors of the lines of π.*

Desarguesian planes

Theorem

For p a prime, $q = p^t$, and $\Pi = PG_2(\mathbb{F}_q)$, $C_p(\Pi)$ is a $[1 + q + q^2, \binom{p+1}{2}^t + 1, q + 1]_p$ p-ary code. The minimum-weight vectors are the scalar multiples of the incidence vectors of the lines. If $\pi = AG_2(\mathbb{F}_q)$, then $C_p(\pi)$ is a $[q^2, \binom{p+1}{2}^t, q]_p$ p-ary code and the minimum-weight vectors are the scalar multiples of the incidence vectors of the lines of π.
The minimum weight of $C_p(\Pi)^\perp$ and of $C_p(\pi)^\perp$ is in the range

$$[q + p, 2q]$$

with equality at the lower bound if $p = 2$.

Binary codes

If a projective plane of even order n does not have hyperovals, the next possible weight in $C_2(\Pi)$ is $n+4$.

A non-empty set $\mathcal{S}$ of points in a plane is of even type if every line of the plane meets it evenly. Then $|\mathcal{S}|$ and the order n of the plane must be even, and that $|\mathcal{S}| = n + 2s$, where $s \geq 1$.

A set of points has type $(n_1, n_2, \ldots, n_k)$ if any line meets it in n_i points for some i, and for each i there is at least one line that meets it in n_i points. A hyperoval is a set of size $n+2$ of type $(0, 2)$.

So the set is of even type if all the n_i are even. If a set $\mathcal{S}$ of size $n+4$ in a plane of even order n is of even type, then it is of type $(0, 2, 4)$.

- Korchmáros and Mazzocca [KM90] consider $(n+t)$-sets of type $(0,2,t)$ in the desarguesian plane of order n. They show that sets of size $n+4$ that are of type $(0,2,4)$ always exist in the desarguesian plane for $n = 4, 8, 16$.
- In Key, McDonough and Mavron [KMM] found, by a search for two disjoint complete 18-arcs with some other special properties, a 36-set of this type for $n = 32$. There are no existence results for size $n+4$ for $n > 32$.
- In Key and de Resmini [KdR98] it is shown that all the known planes of order 16 have 20-sets of even type. (Two of these planes do not have hyperovals.)
- Blokhuis, Szőnyi and Weiner [BSW03], Gács and Weiner [GW03], and Limbupasiriporn [Lim05], further explore sets of even type.

Odd-order planes

The minimum weight of the dual code of planes of odd order is only known in general for desarguesian planes of prime order p (when it is $2p$), and for some planes of small order.
The following results appeared in Clark and Key [CK99], and part of them much earlier in Sachar [Sac79]:

Theorem

If $\mathcal{D}$ is a projective plane of odd order $q = p^t$, then

1. $d^{\perp} \geq \frac{4}{3}q + 2$;
2. *if $p \geq 5$ then* $d^{\perp} \geq \frac{3}{2}q + 2$.

Odd-order planes

The minimum weight of the dual code of planes of odd order is only known in general for desarguesian planes of prime order p (when it is $2p$), and for some planes of small order.
The following results appeared in Clark and Key [CK99], and part of them much earlier in Sachar [Sac79]:

Theorem

If $\mathcal{D}$ is a projective plane of odd order $q = p^t$, then

1. $d^\perp \geq \frac{4}{3}q + 2$;
2. *if $p \geq 5$ then* $d^\perp \geq \frac{3}{2}q + 2$.

(This is better than the bound $p + q$ for desarguesian planes.)

Odd-order planes

The minimum weight of the dual code of planes of odd order is only known in general for desarguesian planes of prime order p (when it is $2p$), and for some planes of small order.
The following results appeared in Clark and Key [CK99], and part of them much earlier in Sachar [Sac79]:

Theorem

If $\mathcal{D}$ is a projective plane of odd order $q = p^t$, then

1. $d^\perp \geq \frac{4}{3}q + 2$;
2. *if $p \geq 5$ then $d^\perp \geq \frac{3}{2}q + 2$.*

(This is better than the bound $p + q$ for desarguesian planes.)

Theorem

A projective plane of square order q^2 that contains a Baer subplane has words of weight $2q^2 - q$ in its p-ary dual code, where $p|q$.

Translation planes

From Clark, Key and de Resmini [CKdR02]:

Theorem

Let Π be a projective translation plane of order q^m where $m = 2$ or 3, $q = p^t$, and p is a prime. Then the dual code of the p-ary code of Π has minimum weight at most

$$2q^m - (q^{m-1} + q^{m-2} + \cdots + q).$$

If Π is desarguesian, this also holds for $m = 4$.

Translation planes

From Clark, Key and de Resmini [CKdR02]:

Theorem

Let Π be a projective translation plane of order q^m where $m = 2$ or 3, $q = p^t$, and p is a prime. Then the dual code of the p-ary code of Π has minimum weight at most

$$2q^m - (q^{m-1} + q^{m-2} + \cdots + q).$$

If Π is desarguesian, this also holds for $m = 4$.

If this construction could be shown to be valid for translation planes of order q^m for any $m \geq 2$, then we would have a general upper bound for the minimum weight of $2q^m - (q^{m-1} + \cdots + q)$.

For the desarguesian plane of order $q = p^m$, where p is a prime, in all cases where the minimum weight of the dual p-ary code is known, and in particular for $p = 2$, or for $m = 1$, or for $q = 9, 25$, the minimum weight is precisely as given in this formula,

$$\boldsymbol{2p^m - (p^{m-1} + p^{m-2} + \cdots + p) = 2p^m + 1 - \frac{p^m - 1}{p - 1}.}$$

Question

Is the minimum weight of the dual code of the p-ary code of the desarguesian plane of order p^m, where p is a prime, given by this formula for all primes p and all $m \geq 1$?

Key, McDonough and Mavron [KMM] (see also Lavrauw, Storme and Van de Voorde [LSdV]), have shown that the dual code of the desarguesian plane of order $q = p^m$ has words of weight

$$2q + 1 - \frac{q-1}{p^t - 1}$$

for all $t|m$, and hence, for the desarguesian plane of order p^m

$$\boldsymbol{d^{\perp} \leq 2p^m + 1 - \frac{p^m - 1}{p - 1}.}$$

Figueroa planes

A similar construction applies to Figueroa planes: see Key and de Resmini [KdR03].

Theorem

Let Φ be the Figueroa plane $\mathrm{Fig}(q^3)$ of order q^3 where $q = p^t$ and p is any prime. Let C denote the p-ary code of Φ. Then $C^\perp$ contains words of weight $2q^3 - q^2 - q$. Furthermore, if $d^\perp$ denotes the minimum weight of $C^\perp$ then

1. $d^\perp = q + 2$ *if* $p = 2$;
2. $\frac{4}{3}q + 2 \leq d^\perp \leq 2q^3 - q^2 - q$ *if* $p = 3$;
3. $\frac{3}{2}q + 2 \leq d^\perp \leq 2q^3 - q^2 - q$ *if* $p > 3$.

Planes of order 9

The other odd orders for which the minimum weight is known in the desarguesian case are $q = 9$ (see [KdR01]) and $q = 25$ (see [Cla00, CHKW03]).
From Key and de Resmini [KdR01]:

Theorem

Let Π be a projective plane of order 9. The minimum weight of the dual ternary code of Π is 15 if Π is Φ, Ω, or Ω^D, and 14 if Π is Ψ.

The four projective planes of order 9 are: the desarguesian plane, Φ, the translation (Hall) plane, Ω, the dual translation plane, Ω^D, and the Hughes plane, Ψ. The weight-15 vectors are from the Baer subplane construction; the weight-14 are from two totally disjoint (share no points nor lines) Fano planes.

Planes of order 25

From Clark, Hatfield, Key and Ward [CHKW03]:

Theorem

If Π is a projective plane of order 25 and C is the code of Π over $\mathbb{F}_5$, then the minimum weight $d^\perp$ of $C^\perp$ is either 42 or 44, or $45 \leq d^\perp \leq 50$.

1. *If Π has a Baer subplane, then $d^\perp = 42, 44$ or 45.*
2. *If $d^\perp = 42$, then a minimum-weight word has support that is the union of two projective planes, π_1 and π_2, of order 4 that are totally disjoint and the word has the form $v^{\pi_1} - v^{\pi_2}$.*
3. *If $d^\perp = 44$ then the support of a minimum-weight word is the union of two disjoint complete 22-arcs that have eleven 2-secants in common.*
4. *If $d^\perp = 45$ then $v^\pi - v^\ell$, where π is a Baer subplane of Π and ℓ is a line of Π that is a line of the subplane, is a minimum-weight word.*

Corollary

The dual 5-ary code of the desarguesian projective plane $PG_2(F_{25})$ has minimum weight 45.

All the known planes of order 25 have Baer subplanes. Czerwinski and Oakden [CO92] found the 21 translation planes of order 25.

Planes of order 49

Work included in the masters project of Fidele Ngwane at Clemson, now in Key and Ngwane [KN]:

Theorem

If C is the 7-ary code of a projective plane of order 49, then the minimum weight of the dual code $C^{\perp}$ is at least 87. Thus, the minimum weight $d^{\perp}$ of $C^{\perp}$ satisfies $88 \leq d^{\perp} \leq 98$. Moreover, $88 \leq d^{\perp} \leq 91$ if the projective plane contains a Baer subplane.

Note that a word of weight 86 that consists of two totally disjoint 2-(43,6,1) designs cannot exist by Bruck-Ryser.
Mathon and Royle [MR95] find that there are 1347 translation planes of order 49.

Totally disjoint sets

Definition

Π is a projective plane of order n, and $p|n$, where p is a prime.

Let $\mathcal{S}_i$ for $i \in \{1, 2\}$ be a set of points of Π that is a $(0, 1, h_i)$-set, where $h_i > 1$. Let $|\mathcal{S}_i| = s_i$.
$\mathcal{S}_1$ and $\mathcal{S}_2$ are **totally disjoint** if

- they have no points in common;
- the h_i-secants to $\mathcal{S}_i$ are exterior to $\mathcal{S}_j$;
- every 1-secant to $\mathcal{S}_i$ is a 1-secant to $\mathcal{S}_j$,

for $\{i, j\} = \{1, 2\}$.

Feasible cases:

1. $s_1 = s_2 = h_1 = h_2$: the configuration consists of two lines with the point of intersection omitted.
2. If $n = q^r = p^t$ and $s_2 = h_2$, then $p|h_1$ and $(h_1 - 1)|(q^r - 1)$ is possible if $h_1 = q$, which will give a word of weight $2q^r - (q^{r-1} + q^{r-2} + \ldots + q)$.

Other numerical possibilities

1. $n = 9$, $s_1 = s_2 = 7$, $h_1 = h_2 = 3$: two absolutely disjoint Fano planes, weight 14 (see [KdR01]).
2. $n = 25$, $s_1 = s_2 = 21$, $h_1 = h_2 = 5$: two absolutely disjoint planes of order 4, weight 42; in general it is unknown if a plane of order 25 can have an embedded plane of order 4.
3. $n = 27$, $s_1 = s_2 = 19$, $h_1 = h_2 = 3$: two absolutely disjoint Steiner triple systems, weight 38; unknown if this is possible.
4. $n = 27$, $s_1 = 25$, $s_2 = 16$, $h_1 = 3$, $h_2 = 6$: 2-$(25, 3, 1)$ and 2-$(16, 6, 1)$ designs, weight 41; no design with the latter parameters can exist by Fisher's inequality.
5. $n = 49$, $s_1 = s_2 = 43$, $h_1 = h_2 = 7$: two absolutely disjoint 2-(43,7,1) designs, i.e. planes of order 6, weight 86, which do not exist, by Bruck-Ryser.
6. $n = 81$, $s_1 = 73$, $s_2 = 46$, $h_1 = 3$, $h_2 = 6$: 2-$(73, 3, 1)$ and 2-$(46, 6, 1)$ designs, weight 119; unknown if a design with the latter parameters exists.

Note

- The desarguesian plane $PG_{2,1}(F_q)$ does not contain subplanes of orders other than those from subfields of F_q, so the configurations for $n = 9$ or 25 (1. and 2. of previous page) cannot exist for the desarguesian case.
- It is conjectured that any non-desarguesian plane contains a Fano plane (see Neumann [Neu55]).
- Not all the known planes of order 25 have been checked for subplanes of order 4, but some are known not to have any; Clark [Cla00] has a survey of the known results.
- There are no known planes of square order that do not contain Baer subplanes.

References


E. F. Assmus, Jr and J. D. Key.
Designs and their Codes.
Cambridge: Cambridge University Press, 1992.
Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).


Aart Blokhuis, Tamás Szőnyi, and Zsuzsa Weiner.
On sets without tangents in Galois planes of even order.
Des. Codes Cryptogr., 29:91–98, 2003.


K. L. Clark, L.D. Hatfield, J. D. Key, and H. N. Ward.
Dual codes of projective planes of order 25.
Adv. Geom., 3:140–152, 2003.


K. L. Clark and J. D. Key.
Geometric codes over fields of odd prime power order.
Congr. Numer., 137:177–186, 1999.

References


K. L. Clark, J. D. Key, and M. J. de Resmini.
Dual codes of translation planes.
European J. Combin., 23:529–538, 2002.


K. L. Clark.
Improved bounds for the minimum weight of the dual codes of some classes of designs.
PhD thesis, Clemson University, 2000.


Terry Czerwinski and David Oakden.
The translation planes of order twenty-five.
J. Combin. Theory, Ser. A, 59:193–217, 1992.


A. Gács and Zs. Weiner.
On $(q+t, t)$-arcs of type $(0, 2, t)$.
Des. Codes Cryptogr., 29:131–139, 2003.

References


J. D. Key and M. J. de Resmini.
Small sets of even type and codewords.
J. Geom., 61:83–104, 1998.


J. D. Key and M. J. de Resmini.
Ternary dual codes of the planes of order nine.
J. Statist. Plann. Inference, 95:229 – 236, 2001.


J. D. Key and M. J. de Resmini.
An upper bound for the minimum weight of dual codes of Figueroa planes.
J. Geom., 77:102–107, 2003.


J. D. Key, T. P. McDonough, and V. C. Mavron.
An upper bound for the minimum weight of the dual codes of desarguesian planes.
Submitted.

References

J. D. Key and F. Ngwane.
The minimum weight of the dual 7-ary code of a projective plane of order 49.
Des. Codes Cryptogr., 44:133–142, 2007.

Gábor Korchmáros and Francesco Mazzocca.
On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q.
Math. Proc. Cambridge Philos. Soc., 108:445–459, 1990.

J. Limbupasiriporn.
Partial permutation decoding for codes from designs and finite geometries.
PhD thesis, Clemson University, 2005.

References


M. Lavrauw, L. Storme, and G. Van de Voorde.
On the (dual) code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$.
Submitted.


Rudolf Mathon and Gordon F. Royle.
The translation planes of order 49.
Des. Codes Cryptogr., 5:57–72, 1995.


H. Neumann.
On some finite non-desarguesian planes.
Arch. Math., VI:36–40, 1955.


H. Sachar.
The F_p span of the incidence matrix of a finite projective plane.
Geom. Dedicata, 8:407–415, 1979.