Some open conjectures on codes from planes

J. D. Key

keyj@clemson.edu
www.math.clemson.edu/˜keyj

____

ICM 2014 Satellite Conference
Algebraic Coding Theory Aug. 11 - Aug. 12

Abstract

Abstract

We examine some outstanding open questions regarding the code from the row span over a finite field of an incidence matrix of a finite plane. In particular, we show that

- there are non-desarguesian affine planes of order 16 whose binary codes have words the weight of an affine line but that are not the incident vectors of affine lines (joint work with Ghinelli and de Resmini[GdRK08]);
- the Hall planes of even order provide an infinite class of finite projective planes that satisfy the Hamada-Sachar conjecture that the desarguesian planes have the smallest dimension for planes of a given order. The planes and their duals are not tame.

  (Joint work with McDonough and Mavron[KMM14].)

Introduction

Codes from the row span over a finite field of an incidence matrix of a finite projective plane have an important historical role in that the combinatorial structure of the plane led to the usefulness of their dual codes through the use of majority logic decoding, and the subsequent coincidence of interests of coding theorists and finite geometers in the 1960s.

This coincidence of interests continues to the present day.

For the finite geometers, the codes could be used for classification of planes.

We discuss progress in this classification here.

Terminology

- A t-(v,k,λ) design is an incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ such that $|\mathcal{P}|=v$, every block $B\in\mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
- A 2-$(n^2+n+1,n+1,1)$ design, for $n\geq 2$, is a finite projective plane of order n.
- A $2-(n^2,n,1)$ design obtained from removing a line and all the points on it is an affine plane of order n.
- $PG_2(\mathbb{F}_q)$ is the desarguesian projective plane, i.e. the design of points and 1-dimensional subspaces of the projective 2-space over $\mathbb{F}_q$.

More terminology

- The code $C_F(\mathcal{D})$ of the design $\mathcal{D}$ over F is the space spanned by the incidence vectors of the blocks over F,

$$C_F(\mathcal{D}) = \left\langle v^B \mid B \in \mathcal{B} \right\rangle$$

where $v^{\mathcal{Q}}$ is the incidence vector of a subset $\mathcal{Q}$ of points.

- Equivalently, this is the row span over F of a blocks by points incidence matrix for $\mathcal{D}$.
- For planes of order n take $F = \mathbb{F}_p$ where p is prime and $p \mid n$.
- The hull of a code C or design $\mathcal{D}$ if $C = C_F(\mathcal{D})$, is

$$\mathrm{Hull}(C) = C \cap C^{\perp}$$

.

Well-known facts

For Π any projective plane of order n, $p \mid n$ a prime,

- $C = C_p(\Pi)$ has minimum weight $n+1$;
- the minimum words of C are the scalar multiples of the incidence vectors of the lines;
- $\mathrm{Hull}_p(\Pi) = C \cap C^\perp = \langle v^L - v^M \mid L$ and M lines of $\Pi\rangle$.

(easy to prove [AK92, Theorem 6.3.1]).

For desarguesian planes $\Pi = PG_2(\mathbb{F}_{p^t})$, if $C = C_p(\Pi)$, then

- $\dim(C) = \binom{p+1}{2}^t + 1$;
- $\mathrm{Hull}(C)$ has minimum weight $2p^t$;
- the minimum words of $\mathrm{Hull}(C)$ are $\alpha(v^L - v^M)$, for L, M lines of Π, $\alpha \in \mathbb{F}_p^*$.

(from Delsarte, Goethals and MacWilliams, see [AK92, Chapters 5,6]).

Tame planes

The notion of a **tame plane** was introduced in [AK92, Section 6.9]:

Definition

A projective plane Π of order n is said to be **tame** (or tame at p, where $p \mid n$ is a prime) if

- $\mathrm{Hull}_p(\Pi)$ has minimum weight $2n$;
- the minimum-weight vectors of $\mathrm{Hull}_p(\Pi)$ are precisely the scalar multiples of the differences of the incidence vectors of two distinct lines of Π.

Tame planes

- The desarguesian planes are the only ones known to be tame; many non-desarguesian planes of small order have been shown not to be tame, either because the minimum weight of the hull is not $2n$ (see [GdRK08]) or, more frequently, that there are words of weight $2n$ that are not scalar multiples of the differences of the incidence vectors of two lines.
- We show here that the Hall planes of even order 2^{2t} for $t \geq 2$ are not tame by exhibiting words of weight 2^{2t+1} in the binary hull that are not differences of the incidence vectors of two lines.
  From [KdR98, Corollary 3], this shows that the even order Hall planes and their dual planes are not tame for all even orders $n > 4$.

Hamada-Sachar conjecture

- An outstanding conjecture concerning codes from projective planes is the Hamada-Sachar conjecture [AK92, Conjecture 6.9.1]:

Conjecture

Every projective plane of order p^s, p a prime, has p-rank at least $\binom{p+1}{2}^s + 1$ with equality if and only if it is desarguesian.

- This has been demonstrated computationally for many individual planes of small order.
- We show here that the Hall planes of even order $q = 2^t$ have binary codes with dimension greater than that of the desarguesian plane, i.e. greater than 3^t+1, thus reaffirming the conjecture for an infinite class of planes.

Baer segments

- If Π is a projective plane of square order n^2, a subplane π of Π of order n is called a Baer subplane. Lines of Π meet π in 1 or $(n+1)$ points. If a line of Π meets π in a set δ of $n+1$ points, δ is called a Baer segment.
- A hyperoval in a projective plane of even order n is a set of $n+2$ points such that lines meet the set in 0 or two points.

Hall planes of even order

From Key, McDonough and Mavron [KMM14]:

Proposition

If $q = 2^t$, $t \geq 2$, $\Pi = PG_2(\mathbb{F}_{q^2})$, $\mathcal{H}$ the projective Hall plane of order q^2, then

- $\mathrm{Hull}(C_2(\mathcal{H}))$ *contains words of weight $2q^2$ with support the symmetric difference of two Baer subplanes that intersect in a line;*
- *neither $\mathcal{H}$ nor its dual plane $\mathcal{H}'$ is tame;*
- $\dim(C_2(\mathcal{H})) > \dim(C_2(\Pi)) = 3^{2t} + 1$.

Thus the Hall planes of even order confirm the Hamada-Sachar conjecture.

Hall planes construction

Define the projective Hall plane $\mathcal{H}$ by derivation by Baer segments.

- $\Pi = PG_2(\mathbb{F}_{q^2})$, $q = p^e$, p prime, $\mathcal{L}$ the lines of Π, $\ell_\infty \in \mathcal{L}$;
- δ is a Baer segment of ℓ_∞, $|\delta| = q + 1$;
- $\mathcal{B} = \{\pi \mid \pi \text{ a Baer subplane of } \Pi, \pi \supset \delta\}$, $|\mathcal{B}| = q^2(q + 1)$;
- for $\pi_1, \pi_2 \in \mathcal{B}$,
  $\pi_1 \cap \pi_2 = \delta$ or $\delta \cup \{R\}$, some point R off ℓ_∞.
- For $\pi \in \mathcal{B}$, $\{\pi^* \in \mathcal{B} \mid (\pi \setminus \delta) \cap (\pi^* \setminus \delta) = \emptyset\} \cup \{\pi\}$
  form a set of q^2 subplanes that form a parallel class of lines in the new affine (Hall) plane.
- There are $q + 1$ of these parallel classes of subplanes.

Hall planes $\mathcal{H}$ construction

- $\mathcal{L}_c = \{\ell \in \mathcal{L} \mid \ell \cap \ell_\infty \in \ell_\infty \setminus \delta\}$, $|\mathcal{L}_c| = q^3(q-1)$.
  $\mathcal{L}_o = \{\ell \in \mathcal{L} \mid \ell \cap \ell_\infty \in \delta\}$.
- $\mathcal{A}_c = \{m \setminus \ell_\infty \mid m \in \mathcal{L}_c\}$, affine lines common to Π and $\mathcal{H}$.
- $\mathcal{A}_n = \{\pi \setminus \delta | \pi \in \mathcal{B}\}$, the remaining $q^2(q+1)$ affine lines of $\mathcal{H}$.
- For $\mathcal{H}$, adjoin a line at infinity

  $$\ell_\infty^h = (\ell_\infty \setminus \delta) \cup \{X_i \mid 0 \le i \le q\}$$

  where the X_i correspond to the parallel classes of members of $\mathcal{B}$.
- Lines of $\mathcal{H}$ are $\mathcal{L}_c$, $\mathcal{L}_n = \{(\pi \setminus \delta) \cup \{X_i\} \mid \pi \in \mathcal{B}\}$, and $\{\ell_\infty^h\}$, where X_i corresponds to the parallel class containing π.
- For $m \in \mathcal{L}_o$, $m \setminus \delta$ is an affine Baer subplane of $\mathcal{H}$; if $m_1, m_2 \in \mathcal{L}_o$ and $m_1 \cap m_2 \in \delta$ then these affine planes are disjoint, and in $\mathcal{H}$ they are Baer subplanes that share points only on ℓ_∞^h.

The proof for $q = 2^t$

Lines of Π: $\mathcal{L}_c \cup \mathcal{L}_o \cup \{\ell_\infty\}$; lines of $\mathcal{H}$: $\mathcal{L}_c \cup \mathcal{L}_n \cup \{\ell_\infty^h\}$.
$E = \langle v^\ell \mid \ell \in \mathcal{L}_c \rangle \subseteq C_p(\Pi) \cap C_p(\mathcal{H})$.
Show that for any $R \in \delta$, and for any lines $m_1, m_2 \in \mathcal{L}_o$, and $R \in m_1, m_2$,

$$v^{m_1} - v^{m_2} \in E. \qquad (1)$$

This, and using the fact that Π is tame, proves that

- $\dim(E) = \dim(C_2(\Pi)) - (q+1) = 3^{2t} - 2^t$;
- $\mathcal{H}$ is not tame if $t \geq 2$;
- $\dim(C_2(\mathcal{H})) < \dim(C_2(\Pi)) = 3^{2t} + 1$.

Observation

- Computation with Magma[CSW06, BCP97] indicates that Equation 1 holds for any subset of the line of size $q+1$; in fact if $q=p^t$ then the same is true for any subset on the line of size $p^{t-1}+1$.
- We have only proved it for $q=2^t$ and Baer segments, and the proof uses hyperovals in the dual plane.The analogue for odd q is a word in the dual code with certain properties: work in progress.
- If we can prove Equation (1) for any odd q^2, then all Hall planes will satisfy the Hamada-Sachar conjecture, and would not be tame.

Idea of proof using the dual plane

$\Pi = (\mathcal{P}, \mathcal{L}) = PG_2(\mathbb{F}_{p^t})$ and $C = C_p(\Pi)$.

- Let $w \in C^\perp$, $w(X) = a_X$ for $X \in \mathcal{P}$, so $w = \sum_{X \in \mathcal{P}} a_X v^X$.
- In dual plane Π', using homogeneous coordinates, let $w' = \sum_{X \in \mathcal{P}} a_X v^{X'}$. Then

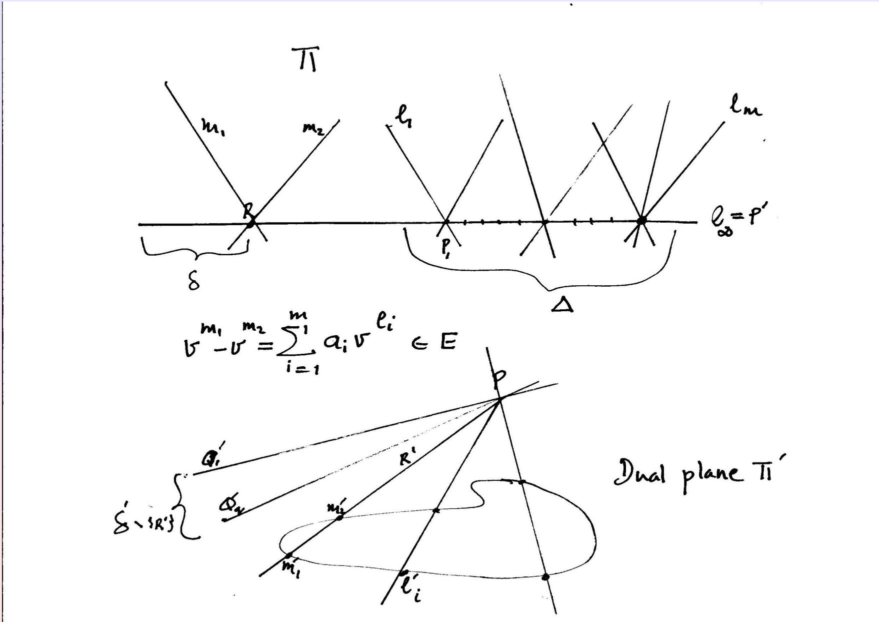
  $$w'(Y) = \sum_{Y \in X'} a_X = \sum_{X \in Y'} a_X = (w, v^{Y'}) = 0$$

  since $w \in C^\perp$. Thus $w' = 0$.
- In particular, if $S = \mathrm{Supp}(w) = \{P_1, \ldots, P_m\}$, where $m = \mathrm{wt}(w)$, and $w(P_i) = a_i \neq 0$, for $i = 1, \ldots, m$, so $w(X) = 0$ for $X \notin S$, then $w' = \sum_{i=1}^m a_i v^{P_i'} = 0$.
- And conversely.

Let $\Pi = PG_2(\mathbb{F}_{q^2})$, δ a chosen set of $q+1$ points on a line $\ell = P'$, and $R \in \delta$. (In particular take δ to be a Baer segment.) Let Δ be the set of points on ℓ that are not in δ.
What we need $w \in C^\perp$ where $S = \mathrm{Supp}(w) = \{P_1, \dots, P_m\}$ and $w(P_i) = a_i \neq 0$, such that:

- $P_1' \cap P_2' = R$, and $a_1 = -a_2$, i.e. $P_1P_2 = R' = P_1P_2P$, i.e. there are two points P_1 and P_2 on S such that the secant ℓ_0 through P_1 and P_2 contains P and is a 2-secant for S, and $\ell_0' = R$;
- for $X \in \delta$, $X \neq R$, the line X' is exterior to S (so at least q of the lines through P are exterior to S);
- for $3 \leq i \leq m$, $P_i' \cap P' = (P_iP)' \in \Delta$, i.e. the other secants through points of S and P are lines ℓ_j where $\ell_j' \notin \delta$.

How it looks


Π
m_1
m_2
ℓ_1
ℓ_m
R
P_1
$\ell_\infty = p'$
δ
Δ
$v^{m_1} - v^{m_2} = \sum_{i=1}^{m} a_i v^{\ell_i} \in E$
P
Q_1'
Q_2'
R'
m_2'
m_1'
ℓ_i'
$\delta' \setminus \{R'\}$
Dual plane Π'

Proof in binary case

In $\Pi = PG_2(q^2)$ where $q = 2^t$, δ a Baer segment:

1. take $\delta \subsetneq \ell_\infty = P'$ where $P \in P'$ (homogeneous coordinates);
2. take $R \in \delta$;
3. find a hyperoval $\mathcal{O}$ in Π such $R \in \mathcal{O}$, $P \notin \mathcal{O}$, and for one secant $\ell \ni P$, $\ell' = R$, but for every other secant m through P, $m' \notin \delta$;
4. if $\ell = P_0Q_0$ and the other secants through P are P_iQ_i for $1 \leq i \leq \frac{q^2}{2}$ then
$$v^{P_0'} + v^{Q_0'} = \sum_{i=1}^{\frac{q^2}{2}} (v^{P_i'} + v^{Q_i'}), \tag{2}$$
and $R = P_0' \cap Q_0'$, where $P_0', Q_0' \in \mathcal{L}_o$, $P_i', Q_i' \in \mathcal{L}_c$ for $i > 0$.

Proof of # 3

For some $z \in K = \mathbb{F}_{q^2}$ let the Baer segment be

$$\delta = \{(1,1,t+z) \mid t \in \mathbb{F}_q\} \cup \{(0,0,1)\},$$

let $R = (0,0,1)$, $P = (1,1,0)$, $\ell_\infty = (1,1,0)'$,

$$\mathcal{O} = \{(1,y,y^{-1}) \mid y \in K^\times\} \cup \{(1,0,0),(0,1,0),(0,0,1)\}.$$

Then $H = \{y^2 + y \mid y \in K\}$ is an additive subgroup of K of order $\frac{q^2}{2}$, and $H > \mathbb{F}_q$.
If we choose $z \notin H$ then the lines $\{(1,1,t+z)' \mid t \in \mathbb{F}_q\}$ are exterior to $\mathcal{O}$.

Proof of # 4

The hyperoval

$$\mathcal{O} = \{P_i, Q_i \mid 0 \le i \le \frac{q^2}{2}\}$$

is such that every line meets it twice or not at all. Thus in the dual plane, the dual hyperoval

$$\mathcal{O}' = \{P_i', Q_i' \mid 0 \le i \le \frac{q^2}{2}\}$$

has the property that every point is on two or none of the lines P_i', Q_i'. Thus

$$\sum_{i=0}^{\frac{q^2}{2}} (v^{P_i'} + v^{Q_i'}) = 0$$

over $\mathbb{F}_2$, proving # 4.

Proof conclusions

- Since P_0', Q_0' meet ℓ_∞ in δ they are Baer subplanes of $\mathcal{H}$ with δ removed, so Equation (2)

$$v^{P_0'} + v^{Q_0'} = \sum_{i=1}^{\frac{q^2}{2}} (v^{P_i'} + v^{Q_i'})$$

  shows that $\mathcal{H}$ is not tame.
- E can be completed to $C_2(\Pi)$ by adding one line through each point of δ, giving the $\dim(E) = \dim(C_2(\Pi)) - (q+1)$.
- $\dim(C_2(\mathcal{H})) > \dim(E) + (q+1)$ since if $\pi_1, \pi_2 \in \mathcal{L}_n$, $\pi_1 \cap \pi_2 = X_0 \in \ell_\infty^h$, then $v^{\pi_1} + v^{\pi_2} \notin E$ since $C_2(\Pi)$ is tame, so $v^{\pi_2} \notin \langle v^{\pi_1}, E \rangle$.

Dimension of code of Hall plane of prime square order

Building up the code of the Hall plane from the code E spanned by the incidence vectors of the lines common to $\mathcal{H}$ and the desarguesian plane, from computational results we found a possiblr formula for the code dimension:

Observation

For p prime, $\mathcal{H}_{p^2}$ the Hall plane of order p^2, $C = C_p(\mathcal{H}_{p^2})$,

$$\dim(C) = \binom{p+1}{2}^2 - p + \sum_{r=2}^{p} \binom{r}{2} + \binom{p}{2} + 1 = \dim(E) + \sum_{r=2}^{p} \binom{r}{2} + \binom{p}{2} + 1.$$

This is verified for $p \leq 11$.

Minimum words in affine planes

From [AK92, Theorem 6.3.3,Corollary 6.4.3]:

Result

- *If π is an affine plane of order n and $p|n$, then* **the minimum weight of $C_p(\pi)$ is n; the minimum-weight vectors are constant.**
- *If Π is a projective plane of order n and $p|n$, such that the minimum weight of $\mathrm{Hull}_p(\Pi) = 2n$, then* **every affine part π of Π has the property that $C_p(\pi)$ has, as minimum-weight vectors, only the scalar multiples of the incidence vectors of the lines of π.**

Planes of order 9 and 16

In[GdRK08] the hulls of all the planes of order 9 and all the known planes of order 16 where computed with Magma [BCP97, CSW06]. This showed:

- All the non-desarguesian planes of these orders are not tame.
- All the non-translation planes of order 16 have hull of minimum weight 24.
- Most of these words of weight 24 yield words of weight 16 in the binary code of some affine plane of order 16 that are not the incidence vectors of affine lines.

Sets of points

A set of points of a plane has type $(n_1, n_2, \ldots, n_k)$ if

- any line meets it in n_i points for some i;
- for each i there is at least one line that meets it in n_i points.

The non-desarguesian planes of order 16

Note: $\dim(C_2(PG_2(\mathbb{F}_{16}))=82$.

Plane		Dim code	Weight		Type	
SEMI2*		98	32		$(0,2,4,8)$	
SEMI4*		98	32		$(0,2,4,8)$	
HALL*	DHALL	98	32	24	$(0,2,4,8)$	$(0,2,8)$
JOWK*	DJOWK	100	32	24	$(0,2,4,8)$	$(0,2,8)$
DEMP*	DDEMP	102	32	24	$(0,2,4,8)$	$(0,2,8)$
LMRH*	DLMRH	106	32	24	$(0,2,4,8)$	$(0,2,8)$
DSFP*	DDSFP	106	32	24	$(0,2,4,8)$	$(0,2,8)$
MATH	DMATH	109	24	24	$(0,2,8)$	$(0,2,8)$
BBH1		110	24		$(0,2,8)$	
BBS4	DBBS4	114	24	24	$(0,2,4)$	$(0,2,8)$
JOHN	DJOHN	114	24	24	$(0,2,8)$	$(0,2,8)$
BBH2	DBBH2	114	24	24	$(0,2,8)$	$(0,2,8)$

Table: Minimum words in the hull of non-desarguesian planes of order 16

Words of weight 16 in affine planes

- All the non-translation projective planes of order 16, apart, possibly, from BBS4, have weight-24 vectors of the type $(0, 2, 8)$ in the hull.
- If $w \in \mathrm{Hull}(\Pi)$, $S = \mathrm{Supp}(w)$, $|S| = 24$, S of type $(0, 2, 8)$ then the three 8-secants meet in a point not in S, the 8-nucleus of the set.
- If ℓ is an 8-secant to S, the affine plane $\pi = \Pi^{\ell}$ formed by taking ℓ as the line at infinity for Π, has $v^{\mathcal{S}\setminus\ell} \in C_2(\pi)$, of weight 16, i.e. with support two sets of eight points on each of two parallel lines.

Conclusion

Computations for orders 25, 27, 32 uncovered more planes that are not tame. E.g., all the non-desarguesian translation planes of order 32 are not tame: each has words of weight 64 in the hull whose support set has type $(0, 2, 4, 16)$.

We do not have an example yet of a non-desarguesian affine plane of odd order n divisible by a prime p whose p-ary code has vectors of weight n that are not the incidence vectors of lines.

(All the planes of order 9 have hulls of minimum weight 18, so we need $n \geq 25$ for an example.)

It might be that

a tame plane must be desarguesian

as was asked in [AK92, page 238].

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).

- W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24, 3/4** (1997), 235–265.

- J. Cannon, A. Steel, and G. White, *Linear codes over finite fields*, Handbook of Magma Functions (J. Cannon and W. Bosma, eds.), Computational Algebra Group, Department of Mathematics, University of Sydney, 2006, V2.13, http://magma.maths.usyd.edu.au/magma, pp. 3951–4023.

- Dina Ghinelli, Marialuisa J. de Resmini, and Jennifer D. Key, *Minimum words of codes from affine planes*, J. Geom. **91** (2008), 43–51.

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

J. D. Key, T. P. McDonough, and V. C. Mavron, *Codes from Hall planes of even order*, J. Geom. **105** (2014), 33–41.