Some open conjectures on linear codes from finite planes

J. D. Key

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

> CIMPA AIMS July 2015

J. D. Key (keyj@clemson.edu)

Codes from planes

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:

- The Hall planes of even order provide an infinite class of finite non-desarguesian 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].)
- There are non-desarguesian affine planes of order 16 that 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].)

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.

- A t-(v, k, λ) design is an incidence structure D = (P, B, I), with point set P, block set B and incidence I such that |P| = v, every block B ∈ B is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
- A 2-(n² + n + 1, n + 1, 1) design, for n ≥ 2, is a projective plane of order n.
- A $2 (n^2, n, 1)$ design obtained by removing a line and all the points on it, from a projective plane is an affine plane of order n.
- $PG_2(\mathbb{F}_q)$ is the desarguesian projective plane, i.e. the design of points and lines of projective 2-space over \mathbb{F}_q ; $AG_2(\mathbb{F}_q)$ is the desarguesian affine plane.

• 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 *D*.
- For planes of order *n* with *p* prime and p|n, take $F = \mathbb{F}_p$.
- The hull of a code C or design \mathcal{D} with $C = C_F(\mathcal{D})$, is

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

.

Well-known facts

For Π any projective plane of order $n, p \mid n, p$ 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;
- $\operatorname{Hull}_{\rho}(\Pi) = C \cap C^{\perp} = \langle v^{L} v^{M} | L \text{ and } M \text{ lines of } \Pi \rangle.$

(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) = $\binom{p+1}{2}^t + 1;$
- Hull(*C*) has minimum weight $2p^t$;
- the minimum words of 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]).

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|n is a prime) if

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

- 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 ≥ 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.

• 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.

- If Π is a projective plane of square order n², 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.

From Key, McDonough and Mavron [KMM14]:

Proposition

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

- Hull(C₂(H)) contains words of weight 2q² having 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.

Define the affine Hall plane \mathcal{AH} and the projective Hall plane \mathcal{H} through derivation by Baer segments.

•
$$\Pi = PG_2(\mathbb{F}_{q^2}), q = p^e, p$$
 prime;

- \mathcal{L} the lines of Π , $\ell_{\infty} \in \mathcal{L}$, $\mathcal{A} = AG_2(\mathbb{F}_{q^2}) = \Pi^{\ell_{\infty}}$;
- δ is a Baer segment of ℓ_{∞} , $|\delta| = q + 1;$
- B = {π | π a Baer subplane of Π, π ⊃ δ}, |B| = q²(q + 1); for π₁, π₂ ∈ B, π₁ ∩ π₂ = δ or δ ∪ {R}, some point R off ℓ_∞.
- For π ∈ B, {π* ∈ B | (π \ δ) ∩ (π* \ δ) = ∅} ∪ {π} form a set of q² subplanes that will form a parallel class of lines in the new affine (Hall) plane *AH*.
- There are q + 1 of these parallel classes of subplanes.

- $\mathcal{L}_c = \{\ell \in \mathcal{L} \mid \ell \cap \ell_\infty \in \ell_\infty \setminus \delta\}$, projective lines common to Π and \mathcal{H} ; $|\mathcal{L}_c| = q^3(q-1).$
- $\mathcal{L}_o = \{\ell \in \mathcal{L} \mid \ell \cap \ell_\infty \in \delta\}.$
- $\mathcal{L} = \mathcal{L}_c \cup \mathcal{L}_o \cup \{\ell_\infty\}$, the lines of Π .
- $\mathcal{A}_c = \{m \setminus \ell_\infty \mid m \in \mathcal{L}_c\}$, affine lines common to \mathcal{A} and \mathcal{AH} .
- $\mathcal{A}_n = \{\pi \setminus \delta | \pi \in \mathcal{B}\}$, the remaining $q^2(q+1)$ affine lines of \mathcal{AH} .
- $\mathcal{A}_c \cup \mathcal{A}_n$ the lines of the affine Hall plane \mathcal{AH} .

 \bullet For the projective Hall plane $\mathcal H,$ adjoin a line at infinity

$$\ell^h_{\infty} = \{X \mid X \in \ell_{\infty} \setminus \delta\} \cup \{X_i \mid 0 \le i \le q\}$$

where the X_i correspond to the parallel classes of members of \mathcal{B} . • Lines of \mathcal{H} are \mathcal{L}_c , ℓ^h_∞ and

$$\mathcal{L}_n = \{ (\pi \setminus \delta) \cup \{X_i\} \mid \pi \in \mathcal{B} \}$$

where X_i corresponds to the parallel class containing π .

For m∈ L_o, m \ δ is an affine Baer subplane of H;
 if m₁, m₂ ∈ L_o and m₁ ∩ m₂ ∈ δ these planes are disjoint;
 in H they share points only on ℓ^h_∞.

Now take $q = 2^t$. 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 $R \in m_1, m_2$,

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

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

- dim(E) = dim(C₂(Π)) (2^t + 1) = 3^{2t} 2^t;
- \mathcal{H} is not tame if $t \geq 2$;
- $\dim(C_2(\mathcal{H})) > \dim(C_2(\Pi)) = 3^{2t} + 1.$

These are true for any q if Equation (1) holds.

- 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 appears to be 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. We have such a word for q = 3 and the Hall plane of order 9: the difference of two Baer subplanes meeting in a line and a point.
- 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.

Lemma

Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane with a polarity σ . Write $X^{\sigma} = X'$ for $X \in \mathcal{P} \cup \mathcal{L}$. Let p be a prime dividing the order of Π , and $C = C_p(\Pi)$.

If
$$w = \sum_X a_X v^X \in C^{\perp}$$
, then $w' = \sum_X a_X v^{X'} = 0$.

Proof: For $Y \in \mathcal{P}$, the value of w' at Y is

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

since $w \in C^{\perp}$. Thus w' = 0.

Codes from planes

Binary case

In $\Pi = PG_2(q^2)$, $q = 2^t$, δ a Baer segment on $\ell_{\infty} = P'$ (homogeneous coordinates, P a point), and $R \in \delta$:

• find a hyperoval $\mathcal{O} = \{P_i, Q_i \mid 0 \le i \le q^2/2\}$ in Π such $P \notin \mathcal{O}$, and for one secant ℓ through P, $\ell' = R$, but for every other secant m through P, $m' \notin \delta$;

3 since $v^{\mathcal{O}} = \sum_i (v^{P_i} + v^{Q_i}) \in C_2(\Pi)^{\perp}$, then

$$\sum_{i} (v^{P'_{i}} + v^{Q'_{i}}) = 0;$$

(a) if $\ell = P_0 Q_0$ and the other secants through P are $P_i Q_i$ for $1 \le i \le \frac{q^2}{2}$ then

$$v^{P'_0} + v^{Q'_0} = \sum_{i=1}^{\frac{q^2}{2}} (v^{P'_i} + v^{Q'_i}), \qquad (2)$$

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.

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), $\ell_{\infty} = (1, 1, 0)'$,

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

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

- $(1,0,0)' \cap (0,1,0)' = (0,0,1) = R \in \delta;$
- for $y \in K^*$,

$$(1, y, y^{-1})' \cap (1, y+1, (y+1)^{-1})' = (1, 1, y^2 + y)) \notin \delta.$$

$$R = \{(1, y, y^{-1}) | y \in K^{*} \} \cup \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \times = YZ$$

$$S = \{(1, 1, r+2) | t \in F \} \cup \{(0, 0, 1)\}$$

$$R_{0} = \{(1, 1, r+2) | t \in F \} \cup \{(0, 0, 1)\}$$

$$R_{0} = \{(1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(1, 1, 0) = (1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(1, 1, 0) = (1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(1, 1, 0) = (1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(1, 1, 0) = (1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = \{(0, 0, 1) = (1, 1, 0) = (1, 1, y^{2} + y) = (1, y, y^{-1})$$

$$R_{0} = (0, 0, 1) = (1, 1, 0)$$

$$R_{0} = (1, 1, 0)$$

21 / 33

- Since P'_0, Q'_0 meet ℓ_∞ in δ they are Baer subplanes of \mathcal{H} with δ removed, so Equation (2) shows that \mathcal{H} is not tame.
- That the word $v^{m_1} v^{m_2}$, where $m_1 \cap m_2 = R \in \delta$ is in E for a specific pair of lines through a specific point in δ shows that for every point in δ and any pair of lines of Π meeting in that point such a vector will be in E, since all homologies and elations are present, and the stabilizer of δ is transitive on δ .
- Thus *E* can be completed to $C_2(\Pi)$ by adding one line through each point of δ , so

 $\dim(E) = \dim(C_2(\Pi)) - (q+1).$

Proof conclusions continued

- dim $(C_2(\mathcal{H}))$ > dim $(E) + (q + 1) = \dim(C_2(\Pi) \text{ since:}$ if $\pi_1, \pi_2 \in \mathcal{L}_n$, i.e. lines in \mathcal{H} but Baer subplanes in Π , and $\pi_1 \cap \pi_2 = X_0 \in \ell_{\infty}^h$, then $v^{\pi_1} + v^{\pi_2} \notin E$ since Π is tame, so $v^{\pi_2} \notin \langle v^{\pi_1}, E \rangle$.
- The last step can be extended to show

 $\dim(C_2(\mathcal{H})) \geq \dim(C_2(\Pi)) + 2.$

Suggested method for *q* odd

- Let $w = \sum_{i=1}^{m} a_i v^{P_i} \in C^{\perp}$ of weight m > 0.
- $S = \text{Supp}(w) = \{P_i \mid 1 \le i \le m\}.$
- Suppose S has a 2-secant, P_1P_2 , and let $R = (P_1P_2)' = P'_1 \cap P'_2$.
- Need to find P ∈ P₁P₂, P ≠ P₁, P₂ such that there is a Baer segment δ with R ∈ δ ⊂ P' with the condition that (PP_i)' ∉ δ for i ≥ 3, i.e. P' ∩ P'_i ∈ P' \ δ for i ≥ 3.

Then

$$a_1(v^{P'_2}-v^{P'_1})=\sum_{i=3}^m a_iv^{P'_i}.$$

• This is a word in Hull(\mathcal{H}) that is not the difference of two lines of \mathcal{H} .



J. D. Key (keyj@clemson.edu)

Codes from planes

25 / 33

We found a suitable word $w \in C^{\perp}$ where $C = C_3(PG_2(\mathbb{F}_9))$:

$$w = v^{\pi_1} - v^{\pi_2}$$

where π_1, π_2 are Baer subplanes (i.e. $PG_2(\mathbb{F}_3)$) of $PG_2(\mathbb{F}_9)$ that meet in a line (Baer segment) and one point off the line.

This word has suitable 2-secants and gives a word of weight 18 in the hull of the Hall plane \mathcal{H} of order 9 that is not the difference of two lines (of \mathcal{H}).

This also shows that dim $(C_3(\mathcal{H})) \ge 38$. (Actual, by computation, is 41).

The following observation came out of computational results up to p = 11 using the idea of adding incidence vectors of lines to the code *E*, and finding the smallest number that must be added at each stage.

Observation

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

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

(41 for p = 3.)

Codes from 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(π) 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 Hull_p(Π) = 2n, then every affine part π of Π has the property that C_p(π) has, as minimum-weight vectors, only the scalar multiples of the incidence vectors of the lines of π.

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.

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.

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

| Plane | | Dim code | Weight | | Туре | |
|--------|-------|----------|--------|----|--------------|-----------|
| 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

Codes from 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 $w \in \text{Hull}(\Pi)$, S = 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 π = Π^l formed by taking *l* as the line at infinity for Π, has v^{S\l} ∈ C₂(π), of weight 16, i.e. with support two sets of eight points on each of two parallel lines.

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 $n \ge 25$ 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.

J. D. Key (keyj@clemson.edu)