Minimum words of codes from affine planes

D. Ghinelli, M.J. de Resmini and J.D. Key

Abstract. We show that there are non-desarguesian affine planes of order 16 for which the binary codes have vectors of minimum weight that are not the incidence vectors of lines. This is is contrast to the desarguesian case and answers an open question as to the nature of the minimum words of the code of a non-desarguesian affine plane. Further, we show that all the non-translation planes of order 16 have hull of minimum weight smaller than 32, in fact containing words of 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. The search has also shown that all the non-desarguesian planes of order at most 16 are not tame. These results are also in contrast to what is known in the desarguesian case. The results are mainly by computer, using Magma.

Mathematics Subject Classification (2000). Primary 94B05 ; Secondary 51A35.

Keywords. Non-desarguesian planes, codes.

1. Introduction

An early observation in the study of the p-ary codes from a projective plane of order n divisible by p was that the minimum weight of the code is $n+1$ and the minimum words are the scalar multiples of the incidence vectors of the lines. A similar study of the codes of an affine plane of order n again gives the minimum weight as n, the minimum words as constant vectors, but no further deduction regarding the nature of the minimum words, apart from in the desarguesian case (see [1, Chapter 6]). We show here that non-desarguesian affine planes can have other vectors of minimum weight in their codes by exhibiting some such vectors in some of the planes of order 16. These words showed themselves in the process of examining the hulls of the non-desarguesian planes of order 9 and 16, with

We thank John Cannon for completing a number of computations that were not feasible on our smaller machines, in particular for finding the minimum weight of the hull for all the non-translation planes of order 16.

the object of finding out if any of these planes are tame. The concept of a tame projective plane was introduced in [1, Definition 6.9.1] as a tool in the search for a coding-theoretic classification of projective planes. A projective plane of order n is tame at a prime p if the hull of the plane, i.e. the intersection of the code of the plane over $\mathbb{F}_p$ with its dual code, has minimum weight $2n$ and the vectors of weight $2n$ are precisely the scalar multiples of the differences of the incidence vectors of two lines. From work of Delsarte, Goethals and MacWilliams, and quoted in full in[1, Chapters 5,6], it is known that this is true for all desarguesian planes. The possibility that the desarguesian planes are the only tame planes arises.

Here we have examined computationally, using Magma [3, 4], all the non-desarguesian planes of order 9 and 16. We found that none of them are tame. This was done by either exhibiting words of weight $2n$ (for $n = 9$ or 16) in the hull that are not the difference of the incidence vectors of two lines, or, for all of the non-translation planes of order 16, finding that the hull has words of weight 24, i.e. less than 32, the known upper bound for the minimum weight of the hull. Further, due to the nature of almost all of these words of weight 24, we found that by choosing a line that intersects the support set of the weight-24 vector suitably, and taking this as the line at infinity, the resulting vector in the affine plane is a vector of weight 16 that is not an incidence vector of an affine line. This provides an example for [1, page 213] or [2, page 10] in the case of affine planes of even order.

The fact that the hull, and hence the code, has vectors of weight less than $2n$, but greater than $n + 1$, also answers another question that is currently being studied, following the work of Chouinard [5, 6]. The question raised there related to the observation that the p-ary code of a desarguesian plane of order $q = p^t$ for some t appeared to have a gap in the weight enumerator between $q + 1$ and $2q$. Chouinard showed that this is always the case for $q = p$, and that it is also true for the three non-desarguesian planes of order 9. Further results for desarguesian planes of order p^2 and p^3 have now been established in [11]. Our findings for the non-translation planes of order 16 show that all of them have words in the hull, and hence in the code itself, in this gap.

We summarize our findings in a proposition:

Proposition 1.1. *Every non-desarguesian projective plane of order* 9 *or* 16 *is not tame. Furthermore, all the non-translation planes of order* 16 *have words of weight* 24 *in their binary hull, and hence also in their code. In this case the minimum weight of the hull is* 24*. Of those planes that have words of weight* 24*, almost all of them have affine parts that have vectors of weight* 16 *in their binary code that are not incidence vectors of affine lines.*

We will exhibit our findings and the nature of the words in Section 3, and give a reference to a website where the planes and these words can be found, so that the reader may verify the computations regarding the existence of the given words in the hull. In Section 2 we will give the definitions and the background results, including some general results for non-tame planes.

2. Background and terminology

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, 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. We write $PG_{2,1}(\mathbb{F}_q)$ or $PG_2(\mathbb{F}_q)$ for the desarguesian projective plane, i.e. the design of points and 1-dimensional subspaces of the projective space $PG_2(\mathbb{F}_q)$. Similarly, $AG_{m,t}(\mathbb{F}_q)$ will denote the design of points of the affine space $AG_m(\mathbb{F}_q)$ and t-flats, where $t \geq 1$. If $\mathcal{S}$ is a set of points in a plane and if L is a line of the plane that meets $\mathcal{S}$ in m points, then L will be called an m**-secant** to $\mathcal{S}$. A Baer subplane of a plane Π of square order n^2 is a subset of n^2+n+1 points of Π which is such that lines of Π meet it in 1 or $n+1$ points; the points and the $(n+1)$-secants form a subplane of Π of order n.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field $\mathbb{F}_p$ and the prime must divide the order of the design, i.e. n for a finite plane of order n. If the incidence vector of a subset $\mathcal{Q}$ of points is denoted by $v^{\mathcal{Q}}$, then $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

A linear code over $\mathbb{F}_q$ of length n, dimension k, and minimum weight d, is denoted by $[n, k, d]_q$. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c, and the **weight** of a vector is the size of its support. A **constant word** in the code is a codeword, all of whose coordinate entries are either 0 or 1. The value of c at the coordinate position X will be denoted by $c(X)$. For any code C, the **dual** or **orthogonal** code $C^\perp$ is the orthogonal under the standard inner product, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. The **hull** of a design with code C is $C \cap C^\perp$, written $\mathrm{Hull}(\mathcal{D})$. A binary code is **doubly-even** if all of its codewords have weight divisible by 4. An **automorphism** of a code C is an isomorphism from C to C.

The following is in [1, Theorem 6.3.1]:

Result 2.1. *Let Π be a projective plane of order n and let p be a prime dividing n. Then the minimum-weight vectors of $C_p(\Pi)$ are precisely the vectors of the form av^L, where a is a non-zero scalar and L is a line of Π. Further, $\mathrm{Hull}_p(\Pi) = \langle v^L - v^M \mid L$ and M lines of $\Pi \rangle$.*

The result for affine planes is in [1, Theorem 6.3.3]:

Result 2.2. *If π is an affine plane of order n and p is a prime dividing n, then the minimum weight of $C_p(\pi)$ is n and all minimum-weight vectors are constant.*

A further general result concerning affine planes is [1, Corollary 6.4.3]:

Result 2.3. *If Π is a projective plane of order n and p is a prime dividing n with 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.*

The situation for the codes from desarguesian planes is quoted in [1, Theorem 6.4.2]:

Result 2.4. *Let p be any prime, $q = p^t$, and $\Pi = PG_2(\mathbf{F}_q)$. Then $C_p(\Pi)$ is a $[q^2+q+1, \binom{p+1}{2}^t + 1, q+1]_p$ code. The minimum-weight vectors of $C_p(\Pi)$ and of $C_p(\Pi) + C_p(\Pi)^\perp$ are the scalar multiples of the incidence vectors of the lines. The minimum weight of $\mathrm{Hull}_p(\Pi)$ is $2q$ and its minimum-weight vectors are the scalar multiples of the differences of the incidence vectors of distinct lines of Π.*

If $\pi = AG_2(\mathbf{F}_q)$, then $C_p(\pi)$ is a $[q^2, \binom{p+1}{2}^t, q]_p$ code. The minimum weight of both $C_p(\pi)$ and $C_p(\pi) + C_p(\pi)^\perp$ is q, and the minimum-weight vectors of $C_p(\pi)$ are the scalar multiples of the incidence vectors of the lines of π. The minimum weight of $\mathrm{Hull}_p(\pi)$ is $2q$, and the minimum-weight vectors are the scalar multiples of the differences of the incidence vectors of distinct parallel lines in π.

As mentioned in Section 1, codes from projective planes of order n appear to have no vectors of weight k where $n+1 < k < 2n$. This is proved by Chouinard [5] for the planes $PG_2(\mathbb{F}_p)$ where p is prime, and, recently, in [11] for $PG_2(\mathbb{F}_{p^2})$ and $PG_2(\mathbb{F}_{p^3})$. Also it was shown in [6] that the three non-desarguesian planes of order 9 satisfy this.

The notion of a tame plane was introduced in [1, Section 6.9] in connection with a rigidity theorem for a class of projective planes.

Definition 2.5. A projective plane Π of order n is said to be *tame* (or tame at p, where p is a prime dividing n) if $\mathrm{Hull}_p(\Pi)$ has minimum weight $2n$ and the minimum-weight vectors are precisely the scalar multiples of the vectors of the form $v^L - v^M$, where L and M are lines of the plane.

Given a set of points $\mathcal{S}$ in a design $\mathcal{D}$ the intersection numbers associated with $\mathcal{S}$ are the sizes of the intersections of the blocks with $\mathcal{S}$. Thus in a 2-design an arc has intersection numbers from the set $\{0, 1, 2\}$. A non-empty set $\mathcal{S}$ of points in a plane is said to be of *even type* if every line of the plane meets it evenly. It follows that $|\mathcal{S}|$ and the order n of the plane must be even, and that $|\mathcal{S}| = n + 2s$, where $s \geq 1$. The incidence vector of a set of even type is thus clearly in the orthogonal binary code of the plane. More specifically, a set of points will be said to have 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. Thus the set is of even type if all the n_i are even. An arc $\mathcal{S}$ is *complete* if no point can be adjoined without $\mathcal{S}$ losing the property of being an arc. The secants (also called 2-secants) to a complete arc cover all the points of the design. Given a set of points $\mathcal{S}$ in a design $\mathcal{D}$ the intersection numbers associated with $\mathcal{S}$ are the sizes of the intersections of the blocks with $\mathcal{S}$. Thus in a 2-design an arc has intersection numbers from the set $\{0, 1, 2\}$.

The following was proved in [8]:

Result 2.6. *Let Π be a projective plane of even order n and suppose that $\mathcal{S}$ is a complete n-arc in Π. Then the set $\mathcal{T}$ of tangents to $\mathcal{S}$ in the dual plane Π^t has*

incidence vector $w^{\mathcal{T}}$ in the binary hull of Π^t. Furthermore, the vector $w^{\mathcal{T}}$ is not the difference of the incidence vectors of two lines in Π^t.

The Hall plane of order q^2, when $q = 2^m$ and $m \geq 4$, has complete q^2-arcs, by Menichetti [13], and the $2q^2$ tangents to an arc of this type form a set of even type in the dual plane. Using this, the following was obtained in [8]:

Result 2.7. *Every dual Hall plane of even square order n has a vector of weight $2n$ in its binary hull that is not the difference of the incidence vectors of two lines.*

It was mentioned in [1, page 231] that the hull of a translation plane of order q must have minimum weight $2q$, due to the fact that the codes of these planes are inside finite geometry codes over $\mathbb{F}_p$, where q is a power of p, and hence the results of Delsarte *et al.* show that the minimum weight is $2q$. However the nature of the words with respect to the lines of the translation plane is not, in general, known. Thus these planes might not be tame even though they have the correct minimum weight. Non-translation planes might not be tame for this reason or for the reason that they have lower minimum weight (necessarily between $q + 2$ and $2q$).

3. Words in the hull

All our computational findings can be found at www.math.clemson.edu/~keyj under the Magma results, heading "tame search". There are 24 files listed there, three for the non-desarguesian projective planes of order 9, and 21 for the non-desarguesian projective planes of order 16. Each file contains the lines of the relevant plane, and the set of points, usually called $w24$ or $w32$ in the case of order 16, whose incidence vector is in the hull of the plane and which shows that the plane is not tame, or, in addition, that the hull has lower minimum weight.

All the planes of order 9 and all those of order 16 are known: there are four of order 9, and 22 of order 16. 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: see [15, 10].

For the planes of order 16 we will use the notation and labelling of [8]. The planes were originally obtained from the ftp site **cs.uwa.edu.au** in the directory **pub/graphs/planes16** [14]. A more recent site is [16].

3.1. Planes of order 9

Each of these was found to have words of weight 18 in the hull with support set $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$ where $\mathcal{S}_i$, for $i = 1, 2$ is an affine plane $AG_{2,1}(\mathbb{F}_3)$. The set $\mathcal{S}$ is of type $(0, 2, 3, 6)$. The three 6-secants meet the two planes in a parallel class each, and the three lines meet at a point on the line at infinity. The other lines of each of the affine planes are external to the other plane and the three remaining parallel classes for these planes meet the line at infinity at a further three points, so that the four points on that line will form the line at infinity for the Baer subplanes.

The three remaining points on the 6-secants form a further affine subplane $\mathcal{S}_3$ that has the same properties. The tangents to the three planes are shared, i.e. each tangent to the one is a tangent to the other. Then we have, in each case, $v^{\mathcal{S}} = v^{\mathcal{S}_1} - v^{\mathcal{S}_2} \in \mathrm{Hull}(\Pi)$, where Π is the projective plane of order 9, or similarly for any choice of two of the planes $\mathcal{S}_i$. Thus the projective planes are not tame.

Additionally, Chouinard [6] showed that 18 is the minimum weight in each case since he showed that there are no words in the code of weight in the range $11 < k < 18$.

3.2. Planes of order 16

We examined all the 21 non-desarguesian planes of order 16, using the planes as found in [14] and the notation of [16]. Our numbering of the planes that can be found at www.math.clemson.edu/~keyj follows that in [8]. We list our findings in Table 1, where each line corresponds to a plane and its dual plane. The dimension of the code is given, followed by the weight of the word that was found in the hull of the code and the hull of the dual plane, respectively, that showed that the plane is not tame, or, in addition in some cases, that 32 is not the minimum weight. The next column gives the type of the support of the word in the code and the dual plane, respectively. These are just examples and are not claimed to be the only type. In fact some words in the dual Hall plane come from the construction in Result 2.7. The seven non-desarguesian translation planes are listed in the first seven rows of the first column, and necessarily have their hulls of minimum weight 32.

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 1. Words in the hull of non-desarguesian planes of order 16

All the computations were done on the Mac OSX version of Magma, apart from that for DDEMP, the dual Dempwolff plane. We thank John Cannon for showing that the hull of this plane has minimum weight 24 and for obtaining a

word of weight 24 for this plane. We also thank him for showing that 24 is indeed the minimum weight of the hull in all the non-translation planes of order 16, i.e. that none of the hulls have words of weight 20, the next possible weight due to the hulls being doubly-even.

Apart from those in BBS4, all the words of weight 24 that we found have support of type $(0, 2, 8)$, i.e. sets of points of size $n+t$ and type $(0, 2, t)$ where $n = 16$ and $t = 8$. Sets of this type in the desarguesian planes of even order were studied in [9], and in [7]. As discussed in [8], the 8-secants partition the set of points, and it also follows that the 8-secants meet in a point (outside the set), called the 8-nucleus of the set. The incidence vector of such a set is clearly in the dual of the code of the plane, but it is surprising to find it in the hull, and thus in the code. Sets of this type in $PG_2(\mathbb{F}_{16})$ were constructed in [9], but note that there is an error in their description in Theorem 6: the set $\{w_1, \ldots, w_7\} = \{1, \zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^8, \zeta^{10}\}$ will work, but not the one given in the paper.

If the plane has a word w of weight 24 in the hull, and hence in the code, with support of type $(0, 2, 8)$ then, if ℓ is an 8-secant to the support $\mathcal{S}$ of w, the affine plane π formed by taking ℓ as the line at infinity will have the property that $v^{\mathcal{S}\setminus\ell} \in C_2(\pi)$, and this is not the incidence vector of a line. The resulting word in the affine plane is the incidence vector of two sets of eight points on each of two parallel lines. All the non-translation projective planes of order 16, apart, possibly, from BBS4, have weight-24 vectors of the type $(0, 2, 8)$. The support of the words of weight 24 in BBS4 that we found are of type $(0, 2, 4)$ and are the union of two disjoint complete 12 arcs. The two arcs have common tangents (72 of them) and 18 common 2-secants, which form the 4-secants of the union. Thus there is not a 4-nucleus. Of course the translation planes will not have such vectors and must have the hull of minimum weight 32. This proves nothing about their affine parts.

For the seven translation planes, where the minimum weight is known to be 32, words of weight 32 were found that have support sets of type $(0, 2, 4, 8)$. All these sets have four 8-secants that partition the set and meet at a point outside, an 8-nucleus. Apart from the set from SEMI2, the sets are the union of two disjoint affine planes of order 4.

4. Conclusion

Further computations with some planes of order 25, 27 and 32 uncovered some more planes that are not tame. For example, 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 $(0, 2, 4, 16)$. Also, in one of the translation planes of order 27, and in the dual of the Andre plane, a word of weight 54 in the hull was found, of the form $v^{S_1} - v^{S_2}$ where each S_i has size 27 and is a $(0, 1, 3, 9)$ set, each with three 9-secants that are common and meet in a point. T. McDonough [12] has found by computation many more words of this form in the hulls of the non-desarguesian planes of order 25 and 27.

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. None of the planes of order 9 would provide such an example: see [2, page 10].

It might be that a tame plane must be desarguesian, as was asked in [1, page 238]. It does not seem to be feasible to continue a computer search for a non-desarguesian tame plane. Similarly, as regards the gap in the weight enumerator of the code, believed to be a property that holds for all desarguesian planes, it is clear that we cannot expect non-desarguesian planes to share this property.

References

[1] 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).

[2] E. F. Assmus, Jr and J. D. Key. Designs and codes: an update. *Des. Codes Cryptogr.*, 9:7–27, 1996.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235–265, 1997.

[4] J. Cannon, A. Steel, and G. White. Linear codes over finite fields. In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006. V2.13, http://magma.maths.usyd.edu.au/magma.

[5] K. Chouinard. *Weight distributions of codes from planes*. PhD thesis, University of Virginia, 2000.

[6] K. Chouinard. On weight distributions of codes of planes of order 9. *Ars Combin.*, 63:3–13, 2002.

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

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

[9] 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.

[10] C. W. H. Lam, G. Kolesova, and L. Thiel. A computer search for finite projective planes of order 9. *Discrete Math.*, 92:187–195, 1991.

[11] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in $PG(n,q)$ and its dual. *Des. Codes Cryptogr.*, 48:231–245, 2008.

[12] T. P. McDonough. Private communication

[13] Giampaolo Menichetti. q-archi completi nei piani di Hall di ordine $q = 2^k$. *Lincei - Rend. Sc. fis. mat. e nat.*, 56:518–525, 1974.

[14] Tim Penttila, Gordon F. Royle, and M. K. Simpson. ftp site: cs.uwa.edu.au. Directory: pub/graphs/planes16.

[15] T. G. Room and P. B. Kirkpatrick. *Miniquaternion Geometry: an Introduction to the Study of Projective Planes*. Cambridge: Cambridge University Press, 1971.

[16] Gordon F. Royle. The projective planes of order 16. http://people.csse.uwa.edu.au/gordon/remote/planes16/index.html.

Acknowledgment

This work was partially supported by GNSAGA of INDAM and the Università di Roma "La Sapienza" (project: *Gruppi, Grafi e Geometrie*). The research started while the third author was a Visiting Professor at the University of Rome "La Sapienza" in June 2008; she gratefully acknowledges the hospitality and financial support extended to her.

D. Ghinelli, M.J. de Resmini
Dipartimento di Matematica
Universitá di Roma 'La Sapienza'
I-00185 Rome, Italy
e-mail: dina@mat.uniroma1.it, resmini@mat.uniroma1.it

J.D. Key
Department of Mathematics and Applied Mathematics
University of the Western Cape
7535 Bellville, South Africa
e-mail: keyj@clemson.edu