Note di Matematica Vol. 18 - n. 1, 7 1-99 (1998)

A DETERMINATION OF THE WEIGHT ENUMERATOR OF THE CODE OF THE PROJECTIVE PLANE OF ORDER 5

GARY McGUIRE, HAROLD N. WARD[1]

Abstract. *We determine the weight enumerator of the code of the projective plane of order 5 by hand. The main tools used are a version of Gleason's theorem on the enumerators of self-dual codes and geometric descriptions of codewords of low weight. This paper contnins the full details of the companion paper [9] that outlined our results.*

1. INTRODUCTION

In this paper we present a calculation of the weight enumerator of the code over $GF(5)$ of the projective plane of order 5. This paper contains the full details of the companion paper [9] that outlined our results. In particular, we have used the same numbering of sections and proven items.

Up to now, the weight enumerators of the codes of the projective planes of orders 2, 3, 4, and 8 were the only ones known. Those of order 2, 3, and 4 are not hard to find by hand, and that of order 8 was found in 1959 by E. Prange [10], using a computer. Our calculation here for the plane of order 5 did not use a computer. Nevertheless, J. D. Key corroborated our results on a computer, using the program Magma.

Thep-ary code of a projective plane of order n is the $GF(p)$-span of the rows of the incidence matrix of the plane, the rows being indexed by the lines and the columns by the points. This code is interesting only when p divides n [1 Theorem 2.4.1]. Therefore, when we talk of the code of the Desarguesian plane of prime order p, we shall always mean the p-ary code. The study of the binary code of a putative projective plane of order 10 was instrumental in the demonstration of the nonexistence of such a plane [6].

The further sections of the paper are:

(2) Blocking Sets and Codes of Projective Planes
(3) An Application of Gleason's Theorem
(4) Some Notation and Codewords of Weight ≤ 10
(5) Minima1 Codewords of Weights 1 l-14 in $C^{\perp}$
(6) Minima1 Codewords of Weights 11-14 not in $C^{\perp}$
(7) All the Codewords of Weights 1 l-14
(8) The Enumerator Obtained.

Section 2 outlines some general results for projective planes of prime order, p. In Section 3, we explain how a version of Gleason's theorem can be used to obtain the weight enumerator of an extension of the code of the plane of order 5 by knowing the numbers of codewords of weight up through 14. Most of the remainder of the paper involves the calculation of these numbers, organized as the section titles suggest.

[1] Partially supported by NSA grant MDA904-95-H-1040.

An interesting feature of the calculations in Sections 5 to 7 is the geometric characterization of the codewords involved. As the reader will see (and, we hope, enjoy), our discussion has a strong geometric content. Objects such as ovals and quadrangles play a large role in the description of these low weight codewords. A paper by A. Beutelspacher [2] presents some of the fascinating aspects of the plane of order 5 that we have encountered, as well as others, in a more combinatoria1 setting.

Finally, we wish to point out a few things. The passage from the weight enumerator of the extended code (which is calculated first) back to that of the code itself is not trivial, and it is laid out in Section 8. Much of the work in Section 7.4 is done so that this passage can be accomplished. In fact, had we only wanted the enumerator of the extended code, we would not have needed D_{14} and Section 7.4 would be much shorter! It will also be apparent that we have almost obtained the complete weight enumerator of the code. In all our descriptions of words of weight up to 14 we obtain the number of occurrences of each digit in a codeword. But this information does not seem to be enough to determine the rest of the enumerator, because Gleason's theorem does not extend this far. We would need to go up through weight 15 (once again, the complete enumerator can be obtained by using Magma).

2. BLOCKING SETS AND CODES OF PROJECTIVE PLANES

In this section we let C denote the ***p-ary*** code of the Desarguesian projective plane of order ***p,*** where ***p*** is an odd prime. The ***support*** of a codeword c, denoted supp(c), is the set of coordinate positions where c has a nonzero entry. The cardinality of supp(c) is the (Hamming) weight of c, which we denote by w(c). We assume that we have fixed an ordering of the points of the plane $PG_2(p)$, and so we identify supp(c) with a subset of $PG_2(p)$. We also identify a line of the plane with its characteristic vector. The dimension of C is $(p^2 + p + 2)/2$, the minimum weight in C is $p + 1$, and the minimum weight codewords are precisely the scalar multiples of the lines [1 Theorem 6.4.2]. If $C^\perp$ denotes the dual code of C, then $C^\perp \subseteq$ C, the minimum weight of $C^\perp$ is $2p$, the minimum weight codewords in $C^\perp$ are precisely the scalar multiples of differences of two lines, and $C^\perp$ is generated by these minimum weight codewords [1 Theorem 6.3.1].

Because of the last fact, it follows that for any codeword c $\in$ C, the dot product c . ℓ has the same value for every line ℓ. If c $\in$ $C^\perp$, then these dot products c . ℓ are zero, while if c $\in$ C \ $C^\perp$ these dot products are nonzero (and all equal).

Definition. A ***blocking set*** S in a projective plane ***D*** is a subset of ***D*** that meets every line, but does not contain a line.

For the basic theory of blocking sets we refer the reader to [5]. We shall use the following observation often.

Proposition 2.1. ***For any codeword c*** $\in$ ***C*** \ $C^\perp$, *if* supp(c) ***does not*** *contain* ***a*** *line,* ***then*** supp(c) ***is a blocking set.***

Proof. We must show that every line meets supp(c); but this is clear since c . $\ell \neq 0$ for all lines ℓ. □

A blocking set S is said to be *reduced* if no proper subset of S is a blocking set. This is

equivalent to saying that, for each point P in S, there is at least one line that meets S only in P (i.e., there is at least one tangent to S on P). For otherwise we could remove P and obtain a blocking set of smaller size.

Proposition 2.2. *If $c \in \mathbf{C} \setminus C^{\perp}$ and $supp(c)$ does not contain a line, then the blocking set $supp(c)$ is not a reduced blocking set.*

Proof. Suppose S = supp (c) is a reduced biocking set. For each $P \in S$, let ℓ_P be a tangent to S on P. Since c . $\ell_P = \alpha$ (say), for each ℓ_P, we get that all nonzero entries of c are equa1 to α. But $c\,\ell = \alpha$ for all lines ℓ, so choosing ℓ to be a line that meets S in more than one point gives a contradiction. □

It has been shown by Blokhuis [3] that if S is a blocking set in the Desarguesian plane of order p, where p is an odd prime, then $|S| \geq 3(p+1)/2$.

Corollary 2.3. *In the p-ary code of the Desarguesian plane of order p, where p is an odd prime, there are no codewords of weight w for $p+2 \leq w \leq 3(p+1)/2$.*

Proof. Let C be the code in question, and let $c \in$ C be a counterexample of minimal weight w, where $p+2 \leq w \leq 3(p+1)/2$. Since $C^{\perp}$ has minimum weight $2p$ we must hnve $c \in \mathrm{C} \setminus C^{\perp}$. If supp($c$) does not contain a line then we are done by Propositions 2.1 and 2.2 and the result of Blokhuis. But if supp(c) does contain a line ℓ, then $c - \beta\ell$ has weight (strictly) lesa than $w - 1$, for some scalar $\beta \in GF(p)$. Since c was a minima1 counterexample, $c - \beta\ell$ must be a scalar multiple of a line. But this means c is a linear combination of two lines, and such sums have weight at least $2p$. □

Next we shall give the well-known equations for any blocking set that arise from counting in two ways. Let S be a blocking set of size m in a projective plane of order n. Let μ_i be the number of lines that meet S in exactly i points. Double counting gives

$$\sum_{i \geq 0} \mu_i = n^2 + n + 1,$$

$$\sum_{i \geq 0} i\mu_i = m(n+1),$$

$$\sum_{i \geq 0} i(i-1)\mu_i = m(m-1).$$

Note that $\mu_0 = 0$.

A line which meets S in i points will be called an *i-line*. First we observe that if $n \geq 5$, any blocking set S has an i-line with $i \geq 4$. For suppose $\mu_i = 0$ if $i \geq 4$. Then we have three equations in three unknowns μ_1, μ_2, μ_3, and solving the system we see that $\mu_2 < 0$ if $n \geq 5$.

Next let us suppose that $\mu_i = 0$ if $i \geq 5$ (this will be the most common case in the plane of order 5). Then the equations become

$$\mu_1 + \mu_2 + \mu_3 + \mu_4 = n^2 + n + 1,$$

$$PI + 2\mu_2 + 3\mu_3 + 4\mu_4 = m(n+1),$$

$$2\mu_2 + 6\mu_3 + 12\mu_4 = m(m-1).$$

Solving these in terms of μ_4 gives

$$\mu_3 = \frac{m(m-1)}{2} - m(n+1) + (n^2+n+1) - 3\mu_4$$
$$\mu_2 = 3m(n+1) - 3(n^2+n+1) - m(m-1) + 3\mu_4$$
$$\mu_1 = 3(n^2+n+1) + \frac{m(m-1)}{2} - 2m(n+1) - \mu_4.$$

Now let us specialize to the case of a projective plane of order $n = 5$. The equations become

$$\mu_3 = \frac{m(m-13)}{2} + 31 - 3\mu_4 \tag{2.1}$$
$$\mu_2 = 19m - m^2 - 93 + 3\mu_4 \tag{2.2}$$
$$\mu_1 = \frac{m(m-25)}{2} + 93 - \mu_4. \tag{2.3}$$

These equations together with Proposition 2.1 will be used frequently in the sequel.

3. AN APPLICATION OF GLEASON'S THEOREM

From now on, C will be the 5-ary code of the projective plane of order 5. We wish to find the weight enumerator of C. We extend C to a self-dual code by adding a column of 2's to the incidence matrix of the plane, drawing on the fact that $2^2 = -1$. This extended code $\bar{C}$ is a self-dual $[32, 16, 7]$ code over GF(5). We shall determine the weight enumerator of $\bar{C}$, and from it, that of C.

A. M. Gleason was the first to observe that the weight enumerator of any self-dual code over $GF(q)$ satisfies certain algebraic constraints [8]. In particular, when $q = 2, 3$, or 4 (for $q = 4$ one uses Hermitian self-duality), the weights satisfy divisibility conditions. This situation is covered by the Gleason-Pierce theorem [8,11]. Although no divisibility restrictions hold for $GF(5)$, there is a theorem also due to Gleason and Pierce for the Lee weight enumerator; it involves invariants known to Felix Klein [7]. Upon specialization, this theorem has implications for the Hamming weight enumerator laid out in [7].

More precisely, Theorem 7 of [7] (whose history, apparently, is uncertain) states the following: let

$$f(z) = 1 + 4z^2,$$
$$g(z) = z^2 - z^4 - 2z^5 + 2z^6,$$
$$h(z) = 5z^4 - 8z^5 - 10z^6 + 20z^7 + 5z^8 - 20z^9 + 8z^{10}.$$

Then the inhomogeneous weight enumerator of any self-dual code over $GF(5)$ is an element of the ring

$$\mathbf{C}[f, \mathrm{SI}] \oplus h\mathbf{C}[f, \mathrm{SI}] \oplus h^2\mathbf{C}[f, g].$$

Let $\bar{A}(z) = \sum_{i=0}^{32} \bar{A}_i z^i$ denote the weight enumerator of $\bar{C}$, $\bar{A}_i$ being the number of codewords of weight i. Then the theorem cited implies that we may write

$$\bar{A}(z) = \sum_{i=0}^{5} a_i f^{16-3i} g^i + h \sum_{i=0}^{3} a_{i+6} f^{11-3i} g^i + h^2 \sum_{i=0}^{2} a_{i+10} f^{6-3i} g^i,$$

for some collection of coefficients $a_0, \ldots, a_{12}$. Expanding the right side and equating the coefficients gives 33 equations connecting the $\bar{A}_i$ and the a_i. The omission of the z term in f and the z^3 term in g implies that $\bar{A}_1 = \bar{A}_3 = 0$. (In coding terms, $\bar{A}_1 = 0$ is obvious, and $\bar{A}_3 = 0$ reflects the fact that no sum of three nonzero squares in $GF(5)$ is 0.) It follows that the best one could hope for, as regards finding the a_i's in terms of the $\bar{A}_i$'s, is that $\bar{A}_0, \ldots, \bar{A}_{14}$ determine the a_i's. This turns out to be the case. In Sections 4 to 7 we shall determine $\bar{A}_0$ to $\bar{A}_{14}$, describing the corresponding codewords in C geometrically. Then in Section 8 we shall evaluate $\bar{A}(z)$ and obtain the enumerator $A(z)$ of C from $\bar{A}(z)$.

4. SOME NOTATION AND CODEWORDS OF WEIGHT ≤ 10

In this section we set up some notation for the rest of the paper and determine all codewords in C of weight 10 or less.

Let A_i denote the number of codewords in C of Hamming weight i. Similarly, let B_i and D_i denote the number of codewords of Hamming weight i in $C^\perp$ and C \ $C^\perp$, respectively. Then

$$A_i = B_i + D_i.$$

Recall that $\bar{A}_i$ denotes the number of codewords of weight i in the extended code $\bar{C}$. All the lines are extended by the same digit, 2, and so the differences of two lines (which generate $C^\perp$) are extended by zero. Therefore all codewords in $C^\perp$ are extended by zero. Since any codeword in C \ $C^\perp$ can be written as the sum of an element of $C^\perp$ and a scalar multiple of the all-1 word, we see that all codewords in C \ $C^\perp$ are extended by a nonzero digit. This implies that

$$\bar{A}_i = B_i + D_{i-1}$$

for $1 \leq i \leq 31$, and $\bar{A}_{32} = D_{31}$.

We claim that the following table is true.

i	0	1	2	3	4	5	6	7	8	9	10
B_i	1	0	0	0	0	0	0	0	0	0	1860
D_i	0	0	0	0	0	0	124	0	0	0	0

The entries for B_i, $0 \leq i \leq 10$, follow from the results stated in the second paragraph of Section 2. The entries for D_i, $0 \leq i \leq 6$, follow from the results stated in the first paragraph of Section 2. The entries for D_i, $7 \leq i \leq 9$, follow from Corollary 2.3. It remains to show that $D_{10} = 0$.

Let c be a word of C \ $C^\perp$ of weight 10. If supp(c) contains a line ℓ, then $c - \beta\ell$ has weight ≤ 8, for some $\beta \in GF(5)$. This implies that $c - \beta\ell = \gamma\ell'$ for some line ℓ' and some $\gamma \in GF(5)$. So c is a combination of two lines, but such sums have weight 11 unless $\beta + \gamma = 0$, in which case c is an element of $C^\perp$ of weight 10. This shows that supp(c) does not contain any lines. By Proposition 2.2, supp(c) is a blocking set that is not reduced.

Since any blocking set has size at least 9, supp(c) = $B \cup \{P\}$ where B is a reduced blocking set of size 9. From Cameron [4], such a blocking set is unique. The points of a projective

triangle give us an example of such a blocking set, so we may assume B is a projective triangle. Every point of B has two tangents (to B), so every point of supp(c) has at least one tangent. Arguing as in the proof of Proposition 2.2 gives a contradiction. This proves that $D_{10} = 0$.

5. MINIMAL CODEWORDS OF WEIGHTS 11-14 IN $C^{\perp}$

In this section we shall find all minima1 codewords of weight 11, 12, 13, and 14 in $C^{\perp}$. Two types will appear, of weights 12 and 13.

First we make an important observation. For any codeword c $\in$ C, if supp(c) meets an i-line where $i \geq 5$, or a 4-line with three coefficients equal, then subtracting the appropriate scalar multiple of that line from c leaves us with a codeword of smaller weight. This motivates the following definition.

Definition. A codeword c $\in$ C is said to be *minima1* if c cannot be written as c' + $\beta\ell$ where c' $\in$ C, $w(c') < \mathrm{w(c)}$, $\beta \in GF(5)$, and ℓ is a line.

Since all codewords can be 'built' from minima1 codewords, our working assumption in this section will be that the given codeword is minimal.

Definition. For any codeword c, let $n_i(c)$ be the number of entries in c that are equa1 to i. We call the vector $(n_1(\mathrm{c}), n_2(c), n_3(c), n_4(c))$, which we often write as $n_1(c)n_2(c)n_3(c)n_4(c)$, the *complexion* of c.

Lemma 5.1. *Let $c \in C^{\perp}$ have weight w. Let (n_1, n_2, n_3, n_4) be the complexion of c. Then*

$$(n_1, n_2, n_3, n_4) \equiv \zeta(1,2,3,4) - w(1,1,1,1) \pmod 5$$

*for **some integer** ζ.*

Proof. We have

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 &= w, \\ n_1 + 2n_2 + 3n_3 + 4n_4 &\equiv 0 \pmod 5, \\ n_1 + 4n_2 + 4n_3 + n_4 &\equiv 0 \pmod 5, \end{aligned}$$

where the second relation comes from c . **j** = 0 (**j** denotes the all-1 word) and the third relation comes from c . c = 0. The first and third relations imply $n_1 + n_4 \equiv 3w$ and $n_2 + n_3 \equiv 3w$ (all congruences are modulo 5). Subtracting the first relation from the second gives $n_2 + 2n_3 + 3n_4 \equiv 4w$. Substitution gives $n_3 + 3n_4 \equiv w$. *Now* let $\zeta = n_1 + w$. We get $n_4 \equiv 3w - (\zeta - \mathrm{w}) \equiv 4w - \zeta \equiv 45 - \mathrm{w}$, so $n_3 \equiv \mathrm{w} - 3n_4 \equiv \mathrm{w} - 3(4w - \zeta) \equiv 3\zeta - \mathrm{w}$. Then $n_2 \equiv 3w - n_3 \equiv 2\zeta - w$. □

Given a codeword c $\in$ C, for a line ℓ that meets the support of c, we shall call the coefficients of the points in $\ell \cap$ supp *(c)* the *Zinepattern* of ℓ. In other words, if $\ell \cap$ supp (c) = $\{P_1, \ldots, P_k\}$ and c_i is the entry of c in position P_i, then $c_1 c_2 \ldots c_k$ is called the line pattern of ℓ.

For a minima1 codeword in $C^{\perp}$, the only possible line patterns are 14, 113, 122, 1144, 1234, 23, 334, 244, 2233. (Use the second paragraph of this section.)

5.1. Minima1 Codewords of Weight 13

Lemma *5.2. Let* $c \in C^{\perp}$ *be a minimal codeword of weight* w, *where* $1 \leq w \leq 14$. *Let* $n_i = n_i(c)$ *be the nuntber of entries of c equal to i, for* $1 \leq i \leq 4$. *Let* ζ *be as in Lemma 5.1. If* $\zeta \not\equiv 0 \pmod 5$, *then one* ***of*** *the* n_i *is zero,*

Proof. If $\zeta \not\equiv 0 \pmod 5$, then w $\equiv$ one of $\zeta, 2\zeta, 3\zeta, 4\zeta$, so we can scale c so that $w \equiv \zeta \pmod 5$. Then $n_1 \equiv 0$, $n_2 \equiv$ w, $n_3 \equiv 2w$, $n_4 \equiv 3w \pmod 5$. It is impossible to have $n_1 = 10$ (otherwise c is not minimal), so if $n_1 \neq 0$ we must have $n_1 = 5$.

On a point $P \in$ c with coefficient 2, suppose there are α lines with line pattern 221 (the first coefficient corresponds to P), β lines with line pattern 2134, γ lines with line pattern 23, 6 lines with line pattern 244, and ϵ lines with line pattern 2233.

This implies that $n_1 = \alpha + \beta$, $n_2 = 1 + \alpha + \epsilon$, $n_3 = \beta + \gamma + 2\epsilon$, $n_4 = \beta + 26$. Since $n_1 = 5$ and $n_3 + n_4 \equiv 0 \pmod 5$ we get $\alpha + \beta = 5$ (so $\gamma + 6 + \epsilon = 1$) and it must be that $n_3 + n_4 = 5$. This is $2\beta + \gamma + 2\delta + 2\epsilon = 5$, so $\gamma = 1 \Rightarrow \delta = \epsilon = 0 \Rightarrow \beta = 2 \Rightarrow \alpha = 3$. We conclude that $n_1 = 5$, $n_2 = 4$, $n_3 = 3$, $n_4 = 2$, and CV = 14. This forces the configuration

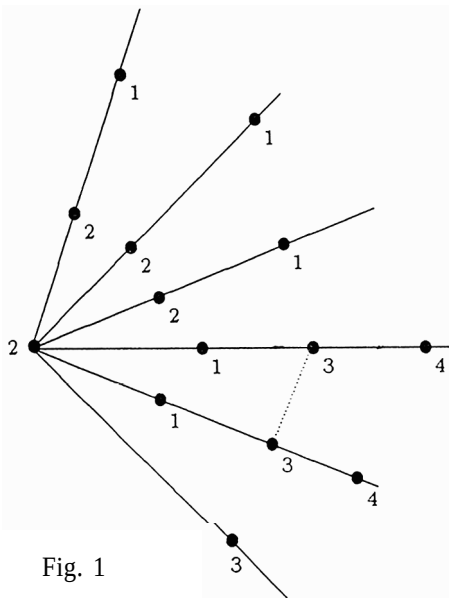

Fig. 1

with respect to any point with coefficient 2. But the dotted line shown must have line pattern 3322, and there are no such lines on a point with coefficient 2 ($\epsilon = 0$). This contradiction proves $n_1 = 0$. cl

Continuing with the assumption that c $\in C^{\perp}$ is a minima1 codeword with $\zeta \not\equiv 0 \pmod 5$, we have shown that we can assume $n_1 = 0$. All of n_2, n_3, n_4 are nonzero. Looking at the set of all possible line patterns emanating from a point P with coefficient 4, we see only two possible line patterns, 433 and 442. Suppose there are α lines with line pattern 433 and $6 - \alpha$ lines with line pattern 442 (the first coefficient corresponds to *P).*

In either case, these lines have two points on them besides P, so $w(c) = 13$. Then $n_3 \equiv 2w \equiv 1 \pmod 5$, so $\alpha = 3$. Therefore $n_1 = 0$, $n_2 = 3$, $n_3 = 6$, $n_4 = 4$.

Consider now the lines on any point with coefficient 2. It follows from the values of the n_i that we have the following configuration.

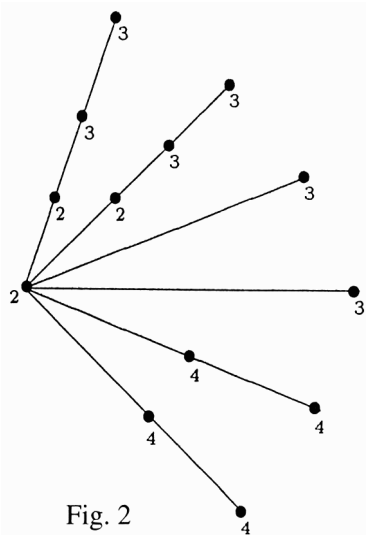

Fig. 2

We refer to a point with coefficient 2 as "a 2", etc. We see that no three of the 4's (points with coefficient 4) are collinear, that is, the 4's are the vertices of a quadrangle. By the above configuration, the three 2's are the intersections of the sides of the quadrangle, that is, the 2's are the diagonal points. On each of the three lines joining two diagonal points there are two points with coefficient 3; these 3's are not on sides.

Codewords with this configuration do exist, as we shall now prove geometrically. The previous paragraph implies that the configuration determines that the support arises from a quadrangle (as explained there). We describe the geometry associated to a quadrangle (the description may be checked routinely by using coordinates).

The 3 1 points of the plane fall into five orbits under the subgroup of the collineation group of the plane permuting the four points (the subgroup is isomorphic to S_4). These orbits will be labeled by letters displayed parenthetically.

The four points are the vertices (V). Pairs of vertices determine six lines, the sides. Opposite sides (not sharing a vertex) meet in one of three diagonal points (D). The diagonal points determine three lines, the diagonals. The sides meet the diagonals in six more points, the harmonic points (H). Each diagonal has two more points not listed so far, giving the six anharmonic points (A). Then the remaining 12 points, the side points (S), lie in twos on the sides.

The harmonic points lie in threes on four lines that form a quadrilateral. The lines of the plane fall into orbits described dually from this quadrilateral, for which the same letters will be used. For example, a V-point is a vertex of the quadrangle, and a V-line a line of the quadrilateral. The D-lines are the diagonals of the quadrangle, and the H-lines are its sides. In the following table, a row shows the number of point-line incidences: Thus each H-line has 2 V-points, and each H-point is on 2 V-lines. The left side numbers reca11 the orbit sizes.

(This symmetry is due to the existence of a correlation exchanging the quadrangle with the quadrilateral.)

		A	D	H	S	V
6	A	1	1	0	4	0
3	0	2	2	2	0	0
6	H	0	1	1	2	2
12	s	2	0	1	2	1
4	V	0	0	3	3	0

As we saw previously, in a conceivable codeword of weight 13 in $C^{\perp}$ each V-point must have coefficient 4, each D-point must have coefficient 2, and each A-point must have coefficient 3. We now show how to obtain such a codeword. Let **h** be the sum of the H-lines and let **s** be the sum of the S-lines. Then

	A	D	H	S	V
h	0	2	1	1	3
s	4	0	2	2	3
h + 2 s	3	2	0	0	4

so we see that **h** + 2 s is such a codeword. The simple count of the number of such codewords is given in Section 5.3.

5.2. Minima1 Codewords of Weight 12

Let c be a minima1 codeword in $C^{\perp}$ of weight w, $11 \leq w \leq 14$. We now assume $\zeta \equiv 0 \pmod 5$ in the conclusion of Lemma 5.1. By Lemma 5.1, $n_1 \equiv n_2 \equiv n_3 \equiv n_4 \equiv -w \pmod 5$. Clearly $w = 11$ leads to a contradiction. If $w = 13$, the only possibility is for one of the n_i to be 7, and the others to equa1 2. By scaling we may assume $n_1 = 7$. Since no three l's can be collinear we must have

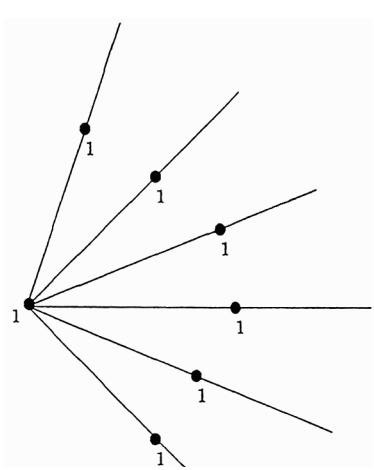

Fig. 3 \

However, examining all the possible line patterns shows that there can be no **2's.** This contradiction eliminates w = 13.

Next we eliminate w = 14. If one of the n_i is equa1 to 11 and the others are equa1 to 1, then there must be three equa1 coefficients on a line, contradicting minimality of c. The other possibility is that two of the n_i are equa1 to 6, the other two equa1 to 1. Scale so that $n_1 = 1$. Let **P** be the point with coefficient 1, and suppose there are α lines on **P** with line pattern 14, β lines on **P** with line pattern 122, γ lines on **P** with line pattern 1234. Then $n_2 = 2\beta + \gamma$, $n_3 = \gamma$, $n_4 = \alpha + \gamma$. It is impossible for two of n_2, n_3, n_4 to equa1 6 and the other to equa1 1.

It remains to consider w = 12. The only possibility is $n_1 = n_2 = n_3 = n_4 = 3$. We shall see that such codewords do exist.

On a point $P \in$ supp (c) with coefficient 1, suppose there are α lines with line pattern 14, β lines with line pattern 113, γ lines with line pattern 122, 6 lines with line pattern 1144, and ϵ lines with line pattern 1234. Then $3 = n_1 = 1 + \beta + 6$, $3 = n_2$ **= 2-y** $+ \epsilon$, **3** = n_3 = $\beta + \epsilon$, $3 = n_4 = \alpha + 2\delta + \epsilon$. Clearly, $\delta = 0$ or 1. If $\delta = 1$, then $\beta = 1 \Rightarrow \epsilon = 2 \Rightarrow n_4 > 3$. So $\delta = 0$, $\beta = 2$, $\epsilon = 1$, $\gamma = 1$, $\alpha = 2$.

The previous paragraph implies that there are three lines intersecting c with line pattern 1234, and that with respect to any point with coefficient 1 the picture is

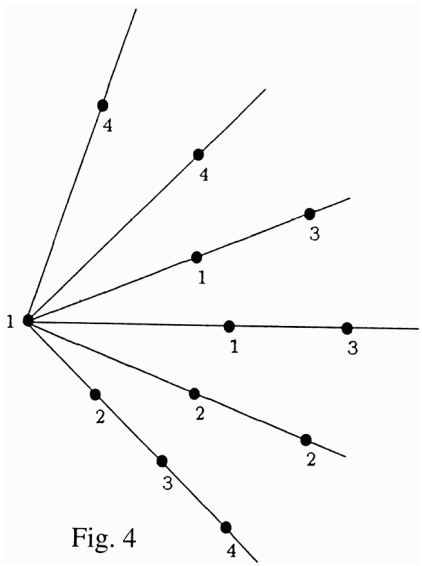

Fig. 4

We claim that these three 1234 lines are concurrent, and meet at a point not in the support of c. For if two of these 1234 lines meet in a point with nonzero coefficient (which cannot be 1 by Figure 4), the same argument as in the previous paragraph leads to a contradiction, since that point has two 1234 lines on it. And if the three 1234 lines meet in three different points with coefficient zero, as shown in Figure 5, we must have

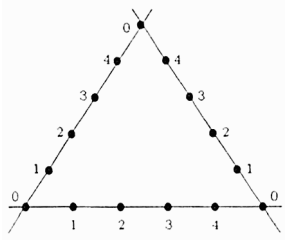

Fig. 5

a triangle, but the line through a vertex and a non-vertex on the opposite side does not hnvc line sum zero. Therefore the picture must be

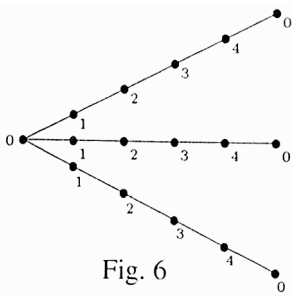

Fig. 6

and the three remaining points with coefficient 0 must be collinear (otherwise the line joining two of them does not have line sum zero).

We shall now construct codewords as in Figure 6. Let D be the Hamming code of length 6 over $GF(5)$. The columns of the parity check matrix for D are the points of $PG_1(5)$. Wc choose

$$H = \begin{bmatrix} 0 & 1 & 4 & 4 & 4 & 4 \\ 1 & 0 & 4 & 3 & 2 & 1 \end{bmatrix},$$

as a parity check matrix for D, so

$$D^{\perp} = \{(b, a, 4b - a, 3b - a, 2b - a, b - a) : a, b \in GF(5)\}.$$

Any two distinct elements of $D^{\perp}$ agree in exactly one place. We can set up the elements of $D^{\perp}$ to be 25 lines in π, the projective plane of order 5. Labe1 the points of π as shown in Figure 7.

We have also shown the six lines L_i through ∞. The remaining 25 lines of π are constructed as follows: the codeword $(x_1, x_2, x_3, x_4, x_5, x_6) \in D^{\perp}$ gives the line which meets L_i at the point on L_i labeled by x_i.

To obtain our codeword c of weight 12, we take the points of L_1, L_2, and L_3 labeled 1, 2, 3, and 4 as the support of c, with the labels as coefficients. Since the first three coordinatcs of any element of $D^{\perp}$ sum to zero (the way we have set it up), we see that $c \in C^{\perp}$.

What we have proved is that codewords of this type are the only codewords of weight 12 in $C^{\perp}$. We can count their number, and we shall do so in Section 5.3.

It would be interesting to know how the weight 12 codewords constructecl above are expressed as a combination of differences of lines. We shall answer this by giving another

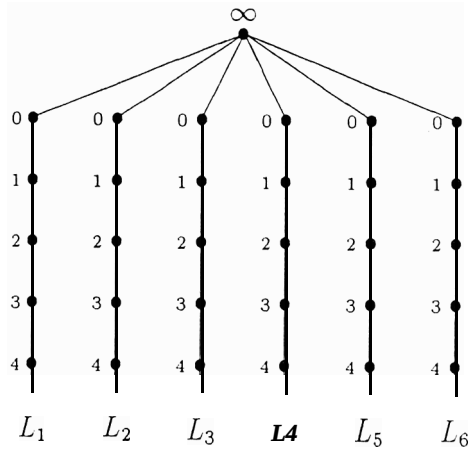

Fig. 7

construction of these codewords. This construction is more interesting geometrically and relates the support of a weight 12 codeword to ovals in the dual projective plane. For this construction we coordinatize the plane. We must pick a line and a point P not on the line, and show that any three points on this given line together with the point P determine the support of a weight 12 codeword in $C^{\perp}$. (In Figure 6, P is the 0 common to the three lines, and the line is the line on the other 0's.)

We choose $P = (0, 0, 1)$ and choose our line to be $z = 0$. We may assume two of the three points on $z = 0$ are $(1, 0, 0)$ and $(0, 1, 0)$, and we scale so that the third point is $(1, 1, 0)$. Let L_1 denote the line $\{(x, y, z) : y = 0\}$, let L_2 denote the line $\{(x, y; z) : x = y\}$, and let L_3 denote the line $\{(x, y, z) : x = 0\}$.

Now choose any point $(1, 1, \alpha)$, $\alpha \neq 0$, on L_2 and construct a sequence of points as follows. We denote the line $ax + by + cz = 0$ by $[a, b, c]$.

Join $(1, 1, \alpha)$ to $(0, 1, 0)$. The line is $[a, 0, -1]$, which meets L_1 at $(1, 0, \alpha) = P_1$.
Join $(1, 0, \alpha)$ to $(1, 1, 0)$. The line is $[\alpha, -\alpha, -1]$, which meets L_3 at $(0, 1, -\alpha) = Q_3$.
Join $(0, 1, -\alpha)$ to $(1, 0, 0)$. The line is $[0, \alpha, 1]$, which meets L_2 at $(1, 1, -\alpha) = P_2$.
Join $(1, 1, -\alpha)$ to $(0, 1, 0)$. The line is $[\alpha, 0, 1]$, which meets L_1 at $(1, 0, -\alpha) = Q_1$.
Join $(1, 0, -\alpha)$ to $(1, 1, 0)$. The line is $[\alpha, -\alpha, 1]$, which meets L_3 at $(0, 1, \alpha) = P_3$.
Join $(0, 1, \alpha)$ to $(1, 0, 0)$. The line is $[0, \alpha, -1]$, which meets L_2 at $(1, 1, \alpha) = Q_2$.

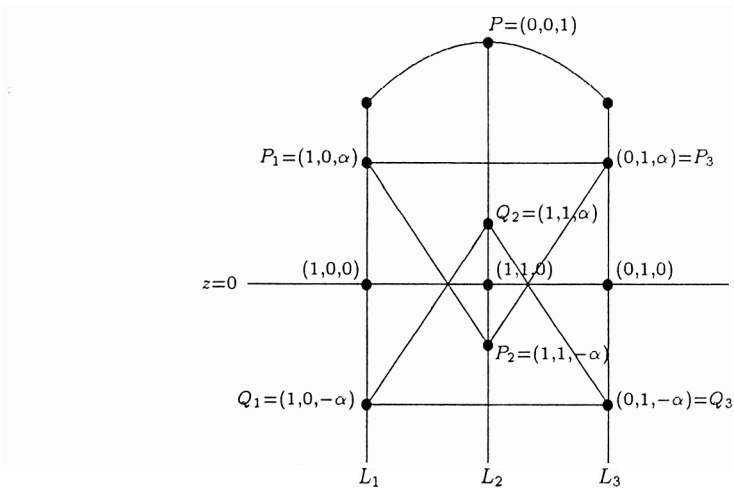

Fig. 8

In each case we 'join' the 'new' point to the one of $(1,0,0)$, $(1,1,0)$, $(0,1,0)$ that it is not already 'joined' to. We have ended back at $(1,1,\alpha)$ after six steps. Note that we could have started by joining $(1,1,\alpha)$ to $(1,0,0)$, and we would get the same six points.

Now form two triangles with the points P_1, P_2, P_3 and Q_1, Q_2, Q_3. This determines six lines, and we claim that these six lines form an oval in the dual plane. To show this, it is a simple matter of checking that the six points in the dual plane lie on the quadric

$$x^2 + xy + y^2 - 3\alpha^2 z^2 = 0.$$

To facilitate things for the reader we give the six points in the dual plane: $P_1P_2 = [-\alpha, 2\alpha, 1]$; $P_1P_3 = [\alpha, \alpha, -1]$; $P_2P_3 = [2\alpha, -\alpha, 1]$; $Q_1Q_2 = [-\alpha, 2\alpha, -1]$; $Q_1Q_3 = [\alpha, \alpha, 1]$; $Q_2Q_3 = [2\alpha, -\alpha, -1]$.

Recall that α is any nonzero element of $GF(5)$. Choosing $\alpha = 1$ or $\alpha = 4$ will result in the same six points $P_1, P_2, P_3, Q_1, Q_2, Q_3$. But choosing $\alpha = 2$ or $\alpha = 3$ will give us another six points, and therefore another oval in the dual plane. Call these six points $R_1, R_2, R_3, S_1, S_2, S_3$, where the R_i is the intersection of L_i with Q_jQ_k, with $j \neq i$, $k \neq i$. Similarly, let $S_i = L_i \cap P_jP_k$. Then a codeword of weight 12 with support $\{P_i, Q_i, S_i, R_i : i = 1,2,3\}$ isgiven by

$$(P_1P_2 + P_1P_3 + P_2P_3) - (Q_1Q_2 + Q_1Q_3 + Q_2Q_3).$$

Each P_i has coefficient 2, each Q_i has coefficient 3, each R_i has coefficient 4 and each S_i has coefficient 1. The six lines involved form an oval in the dual plane. Note that we chose P_iP_j and Q_iQ_j as our six lines. The dual oval formed by the lines R_iR_i and S_iS_i also gives rise to a scalar multiple of the same weight 12 codeword. A further observation is that the same dual oval (with lines P_iP_j and Q_iQ_j, say) can give rise to different codewords of weight 12 by assigning signs differently. Above we assigned $+1$ to the lines P_iP_j and -1 to the lines Q_iQ_j. In all, there are $\binom{6}{3}$ different ways to assign the signs.

In Section 5.3 we shall count the number of these codewords.

We cannot resist making a geometric observation. The six lines in the dual oval are a conic and so no three are concurrent. There are 21 points on the supports of these six lines. It is straightforward to check that the remaining 10 points in the plane form a Desargues configuration!

Remark. We mention here how the above constructions generalize to the Desarguesian plane of order p. The first construction of weight 12 codewords gives codewords of weight $3(p-1)$. The second construction, from ovals in the dual plane, gives codewords of weight $(p+1)(p+3)/4$.

5.3. Counting

In Sections 5.1 and 5.2 we explicitly determined how all minimal codewords of weights 11-14 in $C^{\perp}$ arise. In this section we use **our** descriptions to count the numbers of minimal codewords. We saw that there are no minimal codewords of weights 11 or 14 in $C^{\perp}$.

First let us count weight 12 codewords. We saw that any configuration like

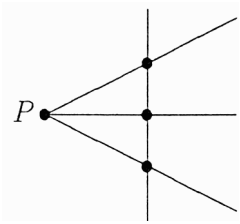

Fig. 9

(with zeros at the four points of intersection) supports a minimal weight 12 codeword (which determines the configuration uniquely). Furthermore, since two such words with the same support can be scaled to agree in at least three places, there is exactly one codeword with this support. (Their difference would be a word in $C^{\perp}$ of weight smaller than 10, but there are no such words.) Therefore we need only count supports and allow for scalar multiples. The number of such codewords is

$$31 \cdot \binom{6}{3} \cdot 25 \cdot 4 = 62,000,$$

where we first choose P, then three lines on P, then the fourth line, and then scale.

We can also arrive at this figure using our second construction, and thereby provide a check. We saw that any oval in the dual plane gives rise to a weight 12 codeword. As in the previous paragraph, we need only count supports and allow for scalars. The number of ovals is easily seen to be 3 100. and so the number of codewords is

$$3100 \cdot \binom{6}{3} \cdot 2 / 2 = 62,000,$$

where we first choose an oval, then assign signs (see Section 5.2), and then scale (there are only two scalar multiples since multiplying by -1 interchanges things). Finally, we divide by 2 because each codeword arises from two dual ovals.

A third way to arrive at this figure is to observe that the automorphism group of the plane (which is $PGL_3(5)$) acts transitively on the configurations of Figure 9. The stabilizer of one of these configurations is isomorphic to $S_3 \times GF(5)^*$, so the number of such configurations is

$$\frac{1}{24}|PGL_2(5)| = \frac{1}{24} \cdot 372,000 = 15,500.$$

Secondly, we shall count the number of minimal codewords of weight 13 in $C^{\perp}$. We showed in Section 5.1 that a quadrangle determines such a codeword, and every such codeword is determined in this way. There is a 1 1 correspondence between supports and quadrangles, because if two such codewords have the same support they can be scaled to agree in at least 4 places and subtracted (again, there are no words in $C^{\perp}$ with weight smaller than 10).

The number of ordered quadrangles is $31 \cdot 30 \cdot 25 \cdot 16$, so the number of minimal codewords of weights 13 in $C^{\perp}$ is

$$4\left(\frac{31 \cdot 30 \cdot 25 \cdot 16}{24}\right) = 62,000,$$

where we multiply by 4 for scalar multiples.

Again, we could view this count in terms of the automorphism group. The group $PGL_3(5)$ is transitive on quadrangles, and the stabilizer of a quadrangle is isomorphic to S_4, so the number of quadrangles is $|PGL_3(5)| / |S_4| = 15{,}500$, giving 62,000 codewords.

Remark. There is in fact a matching of the minimal codewords in $C^\perp$ of weights 12 and 13. It is not hard to see that adding a line and subtracting another line to a weight 12 gives a weight 13. This matching accounts for the numbers of each weight being equal.

6. MINIMAL CODEWORDS OF WEIGHTS 11-14 NOT IN $C^\perp$

The goal of this section is the determination of the codewords in its title. It will turn out that there is only one type, of weight 13.

Let $c \in C \setminus C^\perp$ and scale c to be in the coset $j + C^\perp$, **j** the all-1 word. Then $c \cdot \ell = 1$ for any line ℓ, and $c \cdot c = 1$. Suppose that c is minimal. This restriction on c, along with $c \cdot \ell = 1$, limits the possible line patterns in c to:

$$1,\ 24,\ 33,\ 114,\ 123,\ 222,\ 344,\ 1122,\ 1244,\ 1334,\ 2234.$$

Since an arc in the plane has at most six points [1, Theorem 1.5.1], these line patterns show that each of n_1, n_3, and n_4 is at most 6 (otherwise c is not minimal).

The first claim is that c has no 3. For suppose it did. Of the six lines through a chosen 3, let α have pattern 33; β, 123; γ, 344; δ, 1334; and ϵ, 2234. Then

$$\alpha + \beta + \gamma + \delta + \epsilon = 6, \tag{6.1}$$

and if c has weight w,

$$\alpha + 2\beta + 2\gamma + 3\delta + 3\epsilon = w - 1. \tag{6.2}$$

The condition $c \cdot c = 1$ yields $4 + 4\alpha + 2\gamma + 6 + 4\epsilon \equiv 1 \pmod 5$, or

$$\alpha + \epsilon \equiv 2\gamma + \delta + 3 \pmod 5. \tag{6.3}$$

We also have these equations for the complexion of c:

$$\begin{aligned} n_1 &= \beta + \delta, \\ n_2 &= \beta + 2\epsilon, \\ n_3 &= \alpha + \delta + 1, \\ n_4 &= 2\gamma + \delta + \epsilon. \end{aligned} \tag{6.4}$$

A key point is that equations (6.4), along with (6.1), uniquely determine $\alpha, \beta, \gamma, 6$, and ϵ in terms of the n_i. Thus the counts of line patterns at all the 3's are the same.

Since $n_4 \leq 6$, we have $2\gamma + 6 \leq 6$. Thus, as $\alpha + \epsilon \leq 6$ also, (6.3) implies that

$$\alpha + \epsilon = 2\gamma + \delta + t, \tag{6.5}$$

where either $t = 3$ or $t = -2$. Now solve (6.1), (6.2), and (6.5) for α, β, and γ to get

$$\begin{aligned} \alpha &= \delta + \epsilon + 13 - w, \\ \beta &= -2\delta - 3\epsilon + (t + 3w - 27)/2, \\ \gamma &= \epsilon + (13 - t - w)/2. \end{aligned} \tag{6.6}$$

It must be that $t + w$ is odd. Taking into account the restrictions on the values, we get the following 13 possibilities, tabulated along with the n_i.

		α	β	γ	δ	ϵ				
case	w	33	123	344	1334	2234	n_1	n_2	n_3	n_4
1	112	2	2	0	0	2	2	3		4
2	113	0	2	1	0	1	0	5		5
3	122	3	0	0	1	3	5	3		1
4	123	10		1	1	2	3	5		2
5	123	0	1	0	2	0	4	4		4
6	1	3	0	5	1	0	0	5	5	1	2
7	131	3	1	1	0	4	3	3		3
8	132	11		2	0	3	1	5		4
9	131	2	2	0	1	2	4	2		5
10	13	2	0	2	1	1	1	2	4	6
11	141	3	0	0	2	3	7	2		2
12	14	2	1	0	1	2	2	5	4	3
13	142	0	1	0	3	0	6	3		5

These can all be ruled out by ad-hoc arguments, with some common threads:

Cases 2, 4, 7: n_3 odd, but $6 = 1$, so the 3's can be paired by the 1334 lines.

Cases 5, 9, 10, 12, 13: The 4's in pairs determine $n_4(n_4 - 1)/2$ lines which must have pattems 344 or 1244. The number of 344 lines is γn_3, and the rest are 1244 lines. Various things go wrong. In cases 5 and 13, there are no 1's available. In case 9, at least three of the six 1244 lines must go through one of the two l's, which would force six 4's; and in case 10, the seven 1244 lines would all go through the 1, which is even worse. In case 12, three 1's would be needed for the three 1244 lines (from $n_4 = 3$).

Case 1: The line on the 2's would have to have pattern 1122, there being no 2234. But the two 123 lines show the two 1's and two 2's can't be collinear.

Case 3: The three 2234 lines all have to go through the 4, necessitating six 2's.

Case 6: A line joining a 1 and a 4 must have pattem 114, there being no 1334 and the two 4's determining a 344 rather than a 1244. But the 114 lines through one 4 would pair the five 1's.

Case 8: The 2 would be on five 123 lines (one for each 3), but there are only three 1's.

Case 11: The two 4's would determine a 1244 line, as there is no 344 line. With each of the two remaining l's, a 4 must determine a 114 line, there being no 1334 line. But that would require both 4's to be on the line joining the two 1 's.

Therefore c has no 3's, and the available line pattems drop to 1, 24, 114, 222, 1122, and 1244. There must be 4's. For if not, there would have to be 2's. Suppose a 2 is on α lines with

pattern 222 and $6 - \alpha$ with pattern 1122. Then $c \cdot c = 1$ gives $4 + 3\alpha + 6 - \alpha \equiv 1 \pmod 5$, and $\alpha \equiv 3 \pmod 5$. So $\alpha = 6 - \alpha = 3$, and $w = 16$, too high.

Now take a 4 in c and let α lines through it have pattern 24; β, 114; and γ, 1244. Then $\alpha + \beta + \gamma = 6$, and $c \cdot c = 1$ implies $1 + 4\alpha + 2\beta + \gamma \equiv 1 \pmod 5$. Hence, $\beta \equiv \gamma + 2 \pmod 5$, so that either $\beta = \gamma + 2$ or $\beta = \gamma - 3$. In addition, $w = 1 + \alpha + 2\beta + 3\gamma = 7 + \beta + 2\gamma$. Thus either $w = 3\gamma + 9$ or $w = 3\gamma + 4$. With $11 \leq w \leq 14$, w and γ are pinned down: either $w = 12$ and $\gamma = 1$, or $w = 13$ and $\gamma = 3$. But if $w = 12$, $n_1 = 2\beta + \gamma = 7$, which is too large (c being minimal). So the only possibility is $w = 13$, $\alpha = 3$, $\beta = 0$, $\gamma = 3$, and $n_1 = 3$, $n_2 = 6$, $n_4 = 4$. All four 4's show this arrangement.

There is indeed such a word of weight 13 in C, describable from the quadrangle geometry of Section 5. The 4's must be the vertices of a quadrangle, and the 1244 lines the six sides. Since $n_1 = 3$, the 1's must be the diagonal points. The diagonal lines must have patterns 1122. The six 2's have to be the harmonic points. To see that this prescription really gives a codeword, let d be the sum of the D-lines (diagonals) and v the sum of the V-lines, as before. From the table in Section 5.1 giving point-line incidences, one finds the required word to be **d f v - j .**

The plane contains 15,500 quadrangles (Section 5.3) and thus with scaling allowed, there are 62,000 minima1 codewords of weight 13 not in $C^\perp$.

7. ALL CODEWORDS OF WEIGHT 11-14

In this section we shall determine all codewords in $C^\perp$ and $C \setminus C^\perp$ of weights Il, 12, 13, and 14. In the previous sections we have determined all the minima1 codewords of these weights, and this is our starting point. All other codewords are formed by adding scalar multiples of lines to minima1 codewords. We shall find all possible ways to do this.

7.1. Codewords of Weight 11

Let $c \in C$ be a non-minima1 codeword of weight 11. Then $c = c' + \beta\ell$ where c' has weight less than 11, $\beta \in GF(5)$, and ℓ is a line. From Section 4, c' is either (a scalar multiple of) a line or the difference of two lines, and so c is a linear combination of either two or three lines. Linear combinations of three lines have weight 13, 14, or 15, so $c = \beta\ell + \beta'\ell'$ where $\beta, \beta' \in GF(5)$, and ℓ, ℓ' are lines. Such linear combinations have weight 11 unless $\beta + \beta' = 0$ (in which case the weight is 10). This shows that the number of non-minima1 codewords of weight 11 is $\binom{31}{2} \cdot 3 \cdot 4$, and as explained in Section 4, they all lie in $C \setminus C^\perp$. From Sections 5 and 6 we know that there are no minima1 codewords of weight 1 1. We conclude that

$$B_{11} = 0, \quad D_{11} = \binom{31}{2} \cdot 3 \cdot 4 = 5580.$$

7.2. Codewords of Weight 12

Let $c \in C$ be a non-minima1 codeword of weight 12. Then $c = c' + \beta\ell$ where c' has weight less than 12, $\beta \in GF(5)$, and ℓ is a line. From Section 7.1 and Section 4 we know what c' is: c' must be a linear combination of one or two lines. But then c is a linear combination of two or

three lines. Linear combinations of two lines have weight 10 or 11, and linear combinations of three lines have weight 13, 14, or 15. Hence there are no non-minima] codewords in C of weight 12. We determined the numbers of minima1 codewords of weight 12 in $C^{\perp}$ and $C \setminus C^{\perp}$ in Sections 5 and 6. We conclude that

$$B_{12} = 62{,}000, \quad D_{12} = 0.$$

‘7.3. Codewords of Weight 13

Let $c \in C$ be a non-minima1 codeword of weight 13. Then $c = c' + \beta\ell$ where $w(c') \leq 12$, $\beta \in GF(5)$, and ℓ is a line. From Sections 4, 7.1, and 7.2, we know what the structure of c’ must be. It follows that c is either a linear combination of three lines, or a minima1 codeword of weight 12 plus a scalar multiple of a line.

First let us dea1 with the case that c is a linear combination of three lines. If

$$c = \alpha_1\ell_1 + \alpha_2\ell_2 + \alpha_3\ell_3,$$

where $\alpha_i \in GF(5)$ and ℓ_i is a line, then for c to have weight 13 it is necessary and sufficient that the three lines are not concurrent and exactly two of $\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \alpha_2 + \alpha_3$ are zero. The number of ways to choose three (ordered) non-concurrent lines is 31 . 30 . 25, so the number of codewords is

$$\frac{31 \cdot 30 \cdot 25 \cdot 3 \cdot 4}{3!} = 46{,}500.$$

If $\alpha_1 = \alpha_2 = 1$ and $\alpha_3 = 4$, the complexion is 8104.

Secondly, we consider the case that $c = c' + \beta\ell$ where c’ is a minima1 codeword of weight 12; so $c' \in C^{\perp}$. We shall present c’ by drawing its three 4-lines.

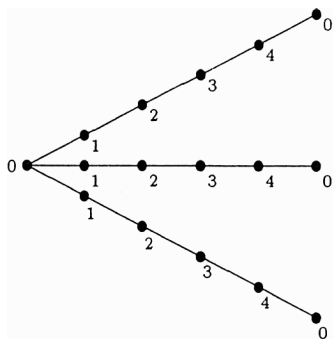

Fig. 10

There are only two ways to add a multiple of a line to c’ and obtain a codeword of weight 13:

(1) Add any multiple of a 4-line,

(2) Add a multiple of a 3-line. The multiple of the 3-line is determined.

For example, we must add 3 times a 122 line in order to get weight 13, because the two points with coefficient 2 must end up with coefficient 0.

It remains to determine how many codewords are constructed by (1) and (2).

(1) There are three 4-lines and we may add any scalar multiple, so we obtain twelve weight 13 codewords in this way from a given weight 12, c'. However, it is possible that a given weight 13 might arise in this way from more than one weight 12. To see if we have overcounted, let us start with a weight 13 codeword c which has been obtained in this way. Without loss of generality we may assume c is

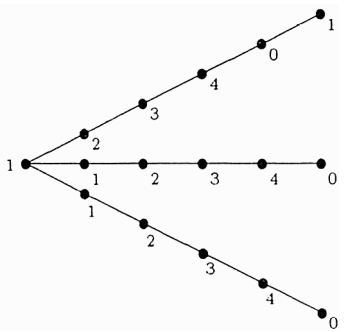

Fig. 11

where the top 4-line has been added to the weight 12 codeword c'. This line is now a 5-line with two coefficients equal. There are three such lines, and any one of them can be subtracted to yield a different minimal weight 12 codeword. Therefore c arises in three ways, and the total number of weight 13 codewords of this type is

$$\frac{62{,}000.\ 12}{3} = 248{,}000.$$

These weight 13 codewords have complexion 4333.

(2) Recall that a minimal weight 12 codeword has twelve 3-lines, which are in three groups of four such that the four lines in each group meet off the support. One group of four lines is shown in Figure 12.

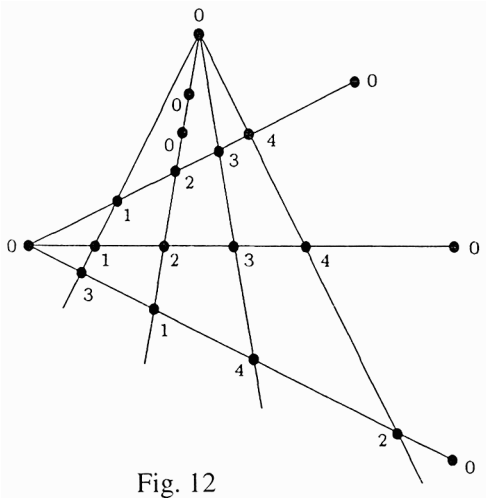

Fig. 12

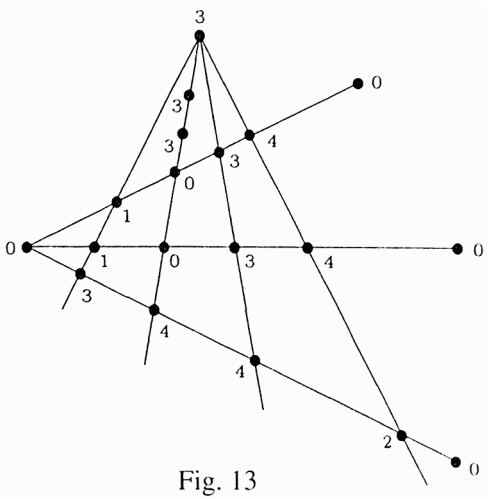

Fig. 13

Suppose we add 3 times the 221 3-line. The resulting weight 13 codeword is shown in Figure 13. Note that the complexion is 2164 and that the 3-line becomes a 4-line with three coefficients equal.

Since there are twelve 3-lines, we obtain twelve weight 13 codewords in this way from one minima1 weight 12 codeword. As in (1), it is possible that a given weight 13 might arise in this way from more than one weight 12. To see if we have overcounted, let us start with a weight 13 as in Figure 13. This codeword has no 5-lines, so the only way to subtract a multiple of a line and lower the weight is to subtract a 4-line with three coefficients equal. How many such lines are there? In general, the three equa1 coefficients will be the scalar which occurs six times, which is 3 in Figure 13. By considering all lines joining two points with coefficient 3, it is not hard to see that there are four lines with line pattern 3334. Therefore our given codeword arises in four ways, and the tota1 number of weight 13 codewords of this type is

$$\frac{62{,}000.\ 12}{4} = 186{,}000.$$

It is clear from the constructions of the sums of three lines and the codewords in (1) and (2), that all of these codewords lie in $C \setminus C^{\perp}$ (they are a multiple of a line added to a member of $C^{\perp}$).

Finally, we can calculate B_{13} and $\boldsymbol{D}_{13}$. Recall from Sections 5 and 6 that there are 62,000 minima1 codewords of weight 13 in $C^{\perp}$, and the same number in $C \setminus C^{\perp}$. Putting all this together gives

$$B_{13} = 62{,}000,$$

$$D_{13} = 46{,}500 + 248{,}000 + 186{,}000 + 62{,}000 = 542{,}500.$$

7.4. Codewords of Weight 14

By the results of Sections 5 and 6, none of the codewords of weight 14 are minimal. One may hope to classify them in terms of the lines which combine with them to lower their weights. The sorting is refined by the complexions.

There are two obvious types of words of weight 14: combinations of three or four lines. A combination of three lines must be a scalar multiple of $\ell_1 + 2\ell_2 + 3\ell_3$, with the ℓ_i three non-concurrent lines. The complexion is 445 1. There is one 6-line, ℓ_1, with pattern 111134, and two 5-lines: ℓ_2, with pattern 22223, and ℓ_3 with pattern 33334. All other lines are 2-lines or 3-lines. Thus the three ℓ_i and their coefficients are determined by the word. There are $3\ 1\ .\ 30 \cdot 25 / 6$ choices for the ℓ_i, 4 choices for the coefficients when scaling is allowed, and 6 ways of assigning them to the ℓ_i, for a tota1 of 93,000 words. These words are not in $C^{\perp}$.

For a combination of four lines, no three of the lines can be concurrent, and the word must be a scalar multiple of a combination $\ell_1 + \ell_2 - \ell_3 - \ell_4$. The word is in $C^{\perp}$, and the complexion is 6116. This word has no 5-line or 6-line, since each ℓ_i is a 4-line. The 1's determine ℓ_1 and ℓ_2, and the 4's determine ℓ_3 and ℓ_4. The ℓ_i form a quadrilatera1 and the number of ways of choosing them is $3\ 1 \cdot 30 \cdot 25 \cdot 16 / 4!$ (as for quadrangles in Sections 5 and 6). The arrangement of signs can be done 6 ways, but scaling only doubles the number: there are 186,000 such words.

We need the complexions of the words of weight 13, and they come from earlier descriptions.

The minima1 13 in $C^{\perp}$ (Section 5.1): 0364.

The minima1 13 in C \ $C^{\perp}$ (Section 6): 3604.

A combination of three lines (Section 7.3): 8 104.

A minima1 12 plus a 4-line (Section 7.3): 4333.

A minima1 12 plus a 3-line (Section 7.3): 2 164.

Scaling produces the cycle (1243) in the complexions.

First we characterize these line combinations.

Proposition 7.1. *Let w(c) = 14 and suppose c has a 6-line. Then c is a combination of three lines.*

Proof. If ℓ is the 6-line, and if ℓ has three equa1 coefficients α, then $8 \leq w(c - \alpha\ell) \leq 11$. By Sections 4 and 7.1, c $- \alpha\ell$ is a combination of two lines and then c is a combination of three.

If ℓ has just a pair of equa1 coefficients α, $w(c - \alpha\ell) = 12$. By Section 7.2, the structure of c $- \alpha\ell$ is that given in Section 5.2. But there is no line ℓ for which adding $\alpha\ell$ to such a word produces a word of weight 14 having ℓ as a 6-line. ✍

Lemma 7.2. *Let $c \in \mathbf{j} + C^{\perp}$, with w(c) = 14. Then modulo 5, c has one of the following complexions:* 0130, 1314, 2043, 3222, 4401.

Proof. Following the pattern in Lemma 5.1, we have

$$\begin{aligned} n_1 + n_2 + n_3 + n_4 &= 14, \\ n_1 + 2n_2 + 3n_3 + 4n_4 &\equiv 1 \pmod 5, \\ n_1 + 4n_2 + 4n_3 + n_4 &\equiv 1 \pmod 5, \end{aligned}$$

the last congruence from $c \cdot c = 1$. Reading the equation modulo 5, we get the five solutions. □

Proposition *7.3. If $c \in \mathbf{j} + C^{\perp}$ and w(c) = 14, then c has either a 5-line or a 6-line.*

Proof. Suppose not. Let μ_i be the number of i-lines of c. By equations (2.1), (2.2), and (2.3), we have $\mu_3 = 38 - 3\mu_4$, $\mu_2 = 3\mu_4 - 23$, and $\mu_1 = 16 - \mu_4$. Thus $8 \leq \mu_4 \leq 12$. A point in the support of c is on at most four 4-lines, but in fact it cannot be on four. For if so, the other two lines through it are a 1-line and a 2-line, and that is inconsistent. Thus $4\mu_4 \leq 3 \cdot 14$, and $\mu_4 \leq 10$. Moreover, a 1 in c cannot be on two 1-lines. Thus from $\mu_1 \geq 6$, there are at least six 1's in c.

The presence of six 1's and the congruences of Lemma 7.2 force the complexion of c to be one of (10)130, 6314, 7043, 8222, or 4444. Because c is not minimal, it must contain a 4-line ℓ with pattern 1113, 2333, or 4444. If ℓ has pattern 4444, $w(c + \ell) = 12$. That would make $c + \ell \in C^{\perp}$ (Section 7.2), and yet $c + \ell$ has coefficient sum 2. This rules out the pattern 4444 for ℓ. So ℓ must contain a 3, and complexion 9401 is eliminated. All the complexions except 6314 have at least seven 1's and therefore a 1113 line. But 6314 cannot have a 2333 line, so it also has a 1113 line. Thus c must have a line ℓ with pattern 1113. In moving to

c − ℓ, the pattern changes from 1113 to 244, the weight goes to 13, and the four remaining complexions change to 7222, 3406, 4135, and 5314.

Only 3406 represents a legitimate word of weight 13 (in $C^{\perp}$). It is one described in Section 5.1, scaled, and is represented (as there) by the following table.

A	D	H	S	V
4	1	0	0	2

The lines in this word with pattern 244 are the S-lines, so ℓ is an S-line. An S-line goes through one H-point, which lies on some D-line. If we add the S-line ℓ to get c, we put a 1 at the H-point. But the D-line was a 4-line, and it becomes a 5-line in c, contrary to assumption. □

Before proceeding, we need the analogue of Lemma 7.2 for $C^{\perp}$, which follows directly from Lemma 5.1:

Lemma 7.4. *Suppose* $c \in C^{\perp}$ *and* $w(c) = 14$. *Then modulo 5, c has one of the complexions* 1111, 2340, 3024, 4203, *or* 0432.

Proposition *7.5. If* $c \in C^{\perp}$ *and* $w(c) = 14$, *then if c contains no 5-line or 6-line, c is a combination offour lines.*

Proof. Once again, c has a 4-line ℓ with three equa1 coefficients, and we may scale c to make the line pattern 3444. Adding ℓ changes the pattern to 114 and changes the weight to 13. Modulo 5, the complexions listed in Lemma 7.4 change as in the following table.

c	$c + \ell$
1111	$c + \ell$
2340	4333
3024	0012
4203	1241
0432	2420

The third and fifth entries for c + ℓ do not correspond to words of weight 13. The first one represents 3604 or 8104; but 8104 is the combination of three lines and would make c the desired combination of four.

In the case of complexion 3604 for c + ℓ, c has complexion 1616. Because $n_1 = n_3 = 1$, the patterns possible for the lines through the 1 are 14, 122, and 1234. There must be exactly one 1234. The rest would have to be 14 to have six 4's. But then there is only one 2, so this case is out.

The second and fourth entries for c + ℓ must represent 4333 and 6241. The corresponding complexions for c are then 2345 and 4253. Scaling, we may assume c has complexion 3524 and a line with pattern either 1112 or 2224.

The possible patterns for the lines through a 1 are 14, 113, 122, 1112, 1144, 1234, and 1333. (Those for other coefficients may be obtained by scaling.) Suppose first that c has a line with pattern 1112. Through a given 1, then, let α lines have pattern 14, β, 122, and

γ, 1234 (the other patterns are missing because all 1's have been used and $n_3 = 2$). Then

$$\begin{aligned} \alpha + \beta + \gamma &= 5, \\ 2\beta + \gamma &= n_2 - 1 = 4, \\ \gamma &= n_3 = 2, \\ \alpha + \gamma &= n_4 = 4. \end{aligned}$$

Thus $\alpha = 2$, $\beta = 1$, and $\gamma = 2$.

It follows that each 3 is on three lines with patterns 1234, one for each 1. There are only two 2's, a 3, and a 4 left for the other three lines through the 3, so their patterns are 23, 23, and 334. Single out that 4 on the line of the two 3's: it is on three lines with patterns 14, again one for each 1. That leaves two lines left through the 4 to accommodate the other eight points in the support of c, and a 5-line or a 6-line is forced (we hope the reader has drawn a diagram!).

Thus we may take it that c has no line with pattern 1112, but it does have one with pattern 2224. If it has two such lines, they meet in a 2. Since all the 2's are on these two lines, the only pattern possible for a line through this 2 and a 1 is 1234. But there would be three such lines and then too many 3's (not to mention too high a weight). So there is one line with pattern 2224.

This time, take a 2 off that line. Of the lines through the 2, let α have pattern 122; β, 23; γ, 2233; 6, 1234; and ϵ, 244. Then

$$\begin{aligned} \alpha + \beta + \gamma + \delta + \epsilon &= 6, \\ \alpha + 6 &= n_1 = 3, \\ \alpha + \gamma &= n_2 - 1 = 4, \\ \beta + 2\gamma + 6 &= n_3 = 2, \\ \delta + 2\epsilon &= n_4 = 5. \end{aligned}$$

This system, however, does not have an integer-valued solution, and we have completed the proof. cl

The remaining possibility for a codeword c of weight 14 is that it has no 6-line, but it does have a 5-line ℓ. If four of the coefficients of c on ℓ are the same, α, then $w(c - \alpha\ell) \leq 11$. From the classification of codewords of weight at most 11, c is a combination of three lines (and thus has a 6-line).

Suppose c has a 5-line ℓ with three (but not four) coefficients the same, α. Then $w(c - \alpha\ell) = 12$, and $c - \alpha\ell$ is one of the words of Section 5.2, with ℓ as a 3-line. Thus such a word c is produced by taking a word t of weight 12, selecting a 3-line ℓ, whose pattern necessarily has the form $(4\alpha)(3\alpha)(3\alpha)$ for some α, and adding $\alpha\ell$. In the resulting word c, ℓ is the only 5-line (the support of c is contained in the union of four lines); and α, the coefficient used, appears on ℓ three times. So the ingredients α, t, and ℓ can be uniquely determined from c. We count the number of these codewords by observing that there are 62,000 choices for t, each having twelve 3-lines. In summary:

Proposition 7.6. *Let c be a codeword of weight* 14 *with a* 5*-line having one coefficient appearing exactly three times. Then c is a combination of a word of weight 12 und one of its*

3-lines. There are 744,000 such words. Their complexions are 1643 (and its scalings), and they are in $C \setminus C^{\perp}$.

Now suppose c has a 5-line ℓ with no coefficient appearing three times. If $c \in C^{\perp}$, we may scale c to make the pattern of ℓ 11224. If $c \notin C^{\perp}$, we scale c to be in $\mathbf{j}+C^{\perp}$. Then ℓ has one of the pattems 11234, 12233, or 23344. If the pattern is 11234, $c - \ell \in C^{\perp}$ and $w(c - \ell) = 13$. In $c - \ell$, ℓ would have pattem 1234. But $c - \ell$ must be one of the minima1 weight 13 words in $C^{\perp}$ from Section 5.1, and these show only three different nonzero coefficients. Thus 11234 is out.

Consider first the case that $c \in C^{\perp}$, ℓ having pattern 11224. As in Proposition 7.5, we list the possible complexions of c modulo 5 and the resulting complexions, also modulo 5, after subtracting ℓ or 21.

c	c - e	c − 21
1111	1421	4022*
2340	2100*	0201*
3024	3334	1430
4203	4013	2114
0432	0242*	3343

If c has a given complexion, both the ones for $c - \ell$ and $c - 21$ must correspond to words of weight 13. The ones marked * do not; so only 3024 and 4203 are possible.

Since c contains 2's on ℓ, however, 3024 must correspond to 3524. Then 1430 in that row corresponds to 1435, which is not the complexion of a word of weight 13. The 4013 in the fourth row could correspond to either 4063 or 4018. But 4018 represents a combination of three lines, making c a combination of four. We have covered that case before Proposition 7.1: c would not have a 5-line. Thus the only possibility remaining is that c has complexion 4253 and $c - \ell$ is a minima1 word of weight 13 with complexion 4063.

In that word of weight 13, ℓ has become a line with pattem 1134. In the quadrangle notation, this word has the same description as the word at the end of Section 6, scaled by 4.

A	*D*	*H*	*S*	*V*
0	4	3	0	1

According to Table 1 in Section 5.1, ℓ must be an *H*-line. The line ℓ is the one joining the two 2's in c, and the scalar multiple by which ℓ is to be subtracted from c is the other duplicated digit on ℓ. There are 15,500 quadrangles, each with 6 H-lines, and 4 scalings are allowed.

Thus we have:

Proposition *7.7. Let* $c \in C^{\perp}$ *and let w(c) =* 14. *Suppose c has no* 6*-line, but that c does have a* 5*-line with no digit appearing three times. Then c is a combination of a minima1 word of weight* 13 *in* $C \setminus C^{\perp}$ *and one of its H-lines. Its complexion is a scaling of 2345. There are* 372,000 *such words.*

Finally, in the remaining case, let $c \in \mathbf{j} + C^{\perp}$ with w(c) = 14, and suppose c has no 6-line, but that c has either a 5-line ℓ with pattern 12233 or a 5-line ℓ' with pattern 23344. We take the possible complexions for c, modulo 5, from Lemma 7.2 and determine the complexions

modulo 5 for the four ways of subtracting a multiple of ℓ or ℓ' to produce a word of weight 13.

c	$c-2\ell$ c - 3 1	$c-3\ell'$	$c-4\ell'$
0130	1 4 2 1	4022*	2114	1020*
1314	2100*	0201*	3343	2204*
2043	3334	1430	4022*	3433
3222	4013	2114	0201*	4112
4401	0242*	3343	1430	0341

Once again, a * marks a complexion modulo 5 that does not correspond to a word of weight 13. Three possibilities remain: complexions 2043 and 3222, modulo 5, with a line ℓ with pattern 12233; and complexion 4401, modulo 5, with a line ℓ' having pattern 23344.

As ℓ' contains 3's in the third case, the actual complexion must be 445 1 and that of $c - 4\ell'$, 5341. But 5341 is not the complexion of a word of weight 13. Similarly, 2043 must correspond to 2543, giving c – 31 the impossible complexion 1435. The 4013 in the remaining case must correspond to 4063, the alternative 40 18 making c a combination of four lines (such a combination for weight 14 has to be in $C^{\perp}$).

Thus it can only be that c has complexion 3272 and c – 2ℓ is exactly the type of minima1 word of weight 13 as in Proposition 7.7. Again ℓ becomes an H-line in c – 2ℓ, but of course we get c by adding 21, not ℓ. The two 2's determine ℓ, and they in turn can be identified as having 2 times the digit that appears three times. Thus ℓ, the coefficient of ℓ in the subtraction, and the codeword of weight 13 are uniquely determined by c. So we get the same number of words as before:

Proposition 7.8. *Suppose $c \in C \setminus C^{\perp}$ and w(c) = 14. Assume that c has no 6-line, but that it does have a 5-line with no digit on it three times. Then c is a comhination of a minimal word of weight 13 in $C \setminus C^{\perp}$ and one of its H-lines. The complexion of c is a scaling* ***of*** *2237, and there are 372,000* ***of*** *these* ***words.***

We summarize these results by giving representative complexions and counts:

1544:	93,000 words in $C \setminus C^{\perp}$
1661 :	186,000 words in $C^{\perp}$
1643 :	744,000 words in $C \setminus C^{\perp}$
2345 :	372,000 words in $C^{\perp}$
2237 :	372,000 words in $C \setminus C^{\perp}$

Thus the totals for words of weight 14 are $B_{14} = 558{,}000$, $D_{14} = 1{,}209{,}000$, and $A_{14} = 1{,}767{,}000$.

8. THE ENUMERATOR OBTAINED

Here is a list of the codeword counts determined in the preceding sections for those weights w for which there are any codewords.

w	A_w	B_w	D_w
0	1	1	0
6	124	0	124
10	1,860	1,860	0
11	5,580	0	5,580
12	62,000	62,000	0
13	604,500	62,000	542,500
14	1,767,000	558,000	1,209,000

In the extension of C to $\bar{C}$, the digit adjoined to a member c of C is $2(c \cdot \mathrm{j})$. Consequently, $\bar{A}_i = B_i + D_{i-1}$ as in Section 4. We thus have the values

$$\begin{array}{llllll} A_0 = 1 & A_{10} = 1{,}860 & \bar{A}_{13} = 62{,}000 \\ A_7 = 124 & A_{12} = 67{,}580 & \bar{A}_{14} = 1{,}100{,}500. \end{array}$$

The $\bar{A}_i$ not displayed for $i \leq 14$ are 0.

Now we solve for the coefficients a_i introduced in Section 3, obtaining the values

$$\begin{array}{llllll} a_0 = 1 & a_4 = 400{,}535/32 & a_8 = 40{,}357/16 \\ a_1 = -64 & a_5 = -15{,}729/8 & a_9 = -2{,}655/2 \\ a_2 = 1{,}264 & a_6 = 16 & a_{10} = 2{,}639/32 \\ a_3 = -16{,}325/2 & a_7 = -959/2 & a_{11} = -3{,}787/8 \\ & & a_{12} = 743/2. \end{array}$$

Then we compute the weight enumerator $\bar{A}(z)$ and see:

$$\begin{array}{llllll} A_0 = 1 & \bar{A}_{11} = 0 & A_{22} = 7{,}608{,}852{,}660 \\ A_1 = 0 & \bar{A}_{12} = 67{,}580 & A_{23} = 12{,}687{,}385{,}500 \\ A_2 = 0 & \bar{A}_{13} = 62{,}000 & A_{24} = 19{,}672{,}786{,}000 \\ A_3 = 0 & \bar{A}_{14} = 1{,}100{,}500 & A_{25} = 24{,}597{,}495{,}724 \\ A_4 = 0 & \bar{A}_{15} = 3{,}494{,}940 & A_{26} = 26{,}928{,}026{,}000 \\ A_5 = 0 & \bar{A}_{16} = 18{,}026{,}500 & A_{27} = 23{,}661{,}618{,}620 \\ A_6 = 0 & \bar{A}_{17} = 60{,}755{,}040 & A_{28} = 17{,}048{,}822{,}000 \\ A_7 = 124 & \bar{A}_{18} = 216{,}318{,}000 & A_{29} = 9{,}318{,}398{,}500 \\ A_8 = 0 & \bar{A}_{19} = 613{,}490{,}000 & A_{30} = 3{,}776{,}625{,}220 \\ A_9 = 0 & \bar{A}_{20} = 1{,}669{,}922{,}880 & A_{31} = 960{,}194{,}000 \\ A_{10} = 1{,}860 & \bar{A}_{21} = 3{,}623{,}466{,}000 & A_{32} = 120{,}980{,}976. \end{array}$$

The reader may have noticed that D_{14} (which took some effort to find!) was not used in these computations. However, $A_{14} = B_{14} + D_{14}$ will be needed in the fina1 computation of the enumerator of C.

To dea1 with the MacWilliams transform more smoothly, we shall switch to homogeneous weight enumerators. Thus the enumerator of C will be written as

$$A = A(x, y) = \sum_{i=0}^{31} A_i x^{31-i} y^i.$$

B is the enumerator of C-r-, and

$$\bar{A} = \sum_{i=0}^{32} \bar{A}_i x^{32-i} y^i$$

is that of $\bar{C}$. With this notation, $D = A - B$.

Let $\mathcal{H}$ be the space of homogeneous polynomials in x and y. Let M be the transformation of $\mathcal{H}$ of order 2 given by the substitution

$$x \to \frac{x + 4y}{\sqrt{5}}, \quad y \to \frac{X - Y}{\sqrt{5}}.$$

The MacWilliams Theorem [8 Chapter 5, Section 6] says that if W is the weight enumeratoi of an $[n, k]$ code over $GF(5)$ and $W^{\perp}$ is the enumerator of the dual code, then

$$W^{\perp} = 5^{-k+n/2} M(W).$$

We shall need a general description of members $H \in \mathcal{H}$ of even degree for which $M(H) = -H$. Its derivation is analogous to those involved in Gleason's theorems [8 Chapter 19, Section 3], and we shall sketch the steps. Let $\tau = (1 + \sqrt{5})/2$, the golden ratio, and let $\tau' = (1 - \sqrt{5})/2$. Then if $u = x - 2\tau' y$ and $v = x - 2\tau y$, $M(u) = u$ and $M(v) = -v$. One may change variables to u and v and conclude that if H has degree $2m$ and $M(H) = -H$, then H is a linear combination of the monomials $(uv)(u^2)^{m-1-i}(v^2)^i$.

Now $u^2 = (x^2 + 4y^2) - 4\tau'(xy - y^2)$, $v^2 = (x^2 + 4y^2) - 4\tau(xy - y')$, and $uv = x^2 - 2xy - 4y^2$. We arrive at

Lemma 8.1. *Let $H \in \mathcal{H}$ and $M(H) = -H$ where H has degree $2m$. Then for suitable coefficients h_i*

$$H = (x^2 - 2xy - 4y^2) \sum_{i=0}^{m-1} h_i (x^2 + 4y^2)^{m-1-i} (xy - y')^i.$$

We have

$$B = 5^{-16+31/2} M(A) = \frac{1}{\sqrt{5}} M(A),$$

by the MacWilliams Theorem. From $\bar{A}_i = B_i + D_{i-1}$ we obtain

$$\begin{aligned} \bar{A} &= xB + yD = xB + y(A - B) \\ &= yA + \frac{(x - y)}{\sqrt{5}} M(A) \\ &= yA + M(yA). \end{aligned}$$

Of course, $M(\bar{A}) = \bar{A}$ (as this shows), so

$$M\left(yA - \frac{1}{2}\bar{A}\right) = -\left(yA - \frac{1}{2}\bar{A}\right).$$

Apply the lemma to $yA - \frac{1}{2}\bar{A}$ and, for transparency, go back to the inhomogeneous polynomials (putting $z = y/x$ and using the same polynomial letters). We get

$$zA(z) - \frac{1}{2}\bar{A}(z) = (1 - 2z - 4z^2) \sum_{i=0}^{15} h_i(1 + 4z^2)^{15-i}(z - z^2)^i,$$

or, with the left side written out and $z - z^2 = z(1 - z)$,

$$\sum_{i=0}^{32}(A_{i-1} - \bar{A}_i/2)z^i = (1 - 2z - 4z^2) \sum_{i=0}^{15} h_i(1 + 4z^2)^{15-i}(1 - z)^i z^i.$$

What is supposed to be transparent is that the equations for the h_i obtained by equating coefficients of z^i on the two sides, for $0 \le i \le 15$, are triangular. Consequently, the h_i are determined by the values of $A_{i-1} - \bar{A}_i/2$ for $0 \le i \le 15$ ***(A-1 = 0). Now*** the need for A_{14} appears! Solving these equations produces

h_0	=	$-1/2$	h_5	=	-1804	h_{10}	= -89,398
h_1	=	0	h_6	=	1,720	h_{11}	= -71,190
h_2	=	28	h_7	=	16,838	h_{12}	= 17,412
h_3	=	52	h_8	=	21,342	h_{13}	= 53,808
h_4	=	-504	h_9	=	-25,794	h_{14}	= -4,246
						h_{15}	= -33,834.

We expand and collect the terms on the right, obtaining $\sum_{i=0}^{32} H_i z^i$, and produce $A_i = H_{i+1} + \bar{A}_{i+1}/2$. The result is the goal of the paper, the weight enumerator of the code of the projective plane of order 5 over GF(5):

A_0	=	1	A_{11}	=	5,580	A_{22}	= 11,506,425,000
A_1	=	0	A_{12}	=	62,000	A_{23}	= 18,365,221,500
A_2	=	0	A_{13}	=	604,500	A_{24}	= 24,062,665,000
A_3	=	0	A_{14}	=	1,767,000	A_{25}	= 27,302,369,724
A_4	=	0	A_{15}	=	11,895,940	A_{26}	= 25,006,057,620
A_5	=	0	A16	=	41,085,540	A_{27}	= 18,607,471,000
A_6	=	124	A_{17}	=	148,242,000	A_{28}	= 10,587,941,500
A_7	=	0	A_{18}	=	465 , 620,000	A_{29}	= 4,408,386,000
A_8	=	0	A_{19}	=	1,279,819,500	A_{30}	= 1,165,216,220
A_9	=	0	A_{20}	=	3,020,794,380	A_{31}	= 151,980,976.
A_{10}	=	1,860	A_{21}	=	6,454,257,660		

Acknowledgements

During our investigations we enjoyed an extended visit from Ed Assmus, whom we wish to thank for his insights. He was hopeful that ovals would be involved somehow, and this has indeed proved to be true. We also thank Kevin Chouinard and John Polhill for helpful discussions.

REFERENCES

[1] Assmus, E. F., Jr., and Key, J. D.: *Designs and their Codes*, Cambridge University Press, Cambridge, 1992.

[2] Beutelspacher, A.: A defense of the honour of an unjustly neglected little geometry, or, a combinatoria1 approach to the projective plane of order five, J. Geom. 30(1987), 182-195.

[3] Blokhuis, A.: On the size of a blocking set in $PG(2, p)$, Combinatorica 14(1994), 11 l-l 14.

[4] Cameron, P.: Four lectures on projective geometry, in *Finire Geometries*, Lecture Notes in Pure and Appl. Math., vol. 103, Dekker, New York, 1985, 27-63.

[5] Hirschfeld, J. P.: *Projective Geometries over Finire Fields,* Oxford University Press, Oxford, 1979.

[6] Lam, C. W. M.: The search fora finite projective plane of order 10, Amer. Math. Monthly 98(1991), 305–318.

[7] Leon, J. S., Pless, V., and Sloane, N. J. A.: Self-dual codes over $GF(5)$, J. Combin. Theory A 32(1982), 178-194.

[8] MacWilliams, F. J., and Sloane, N. J. A.: *The Theory* of *Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[9] McGuire, G., and Ward, H. N.: The weight enumerator of the code of the projective plane of order 5, Geometriae Dedicata.

[10] Prange, E.: The use of coset equivalence in the analysis and decoding of group codes, Electronics Research Directorate, Air Force Cambridge Research Center, June, 1959, Report AFCRC-TN-59- 164.

[11] Sloane, N. J. A.: Self-dual codes and lattices, in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math., vol. 34, Amer. Math. Soc., Providence, 1979; 273-308.

G. McGuire
National University of Ireland
Department of Mathematics
Maynooth Kildare
IRELAND

H. N. Ward
Department of Mathematics
University of Virginia
Charlottesville
VA 22903 3 199