Ternary Codes of Minimum Weight 6 and the Classification of the Self-Dual Codes of Length 20

VERA PLESS, MEMBER, IEEE, N. J. A. SLOANE, FELLOW, IEEE, AND HAROLD N. WARD

Abstract—Self-orthogonal ternary codes of minimum weight 3 may be analyzed in a straightforward manner using the theory of glueing introduced in earlier papers. The present paper describes a method for studying codes of minimum weight 6: the supports of the words of weight 6 form what is called a center set. Associated with each center set is a graph, and all the graphs that can arise in this way are known. These techniques are used to classify the ternary self-dual codes of length 20: there are 24 inequivalent codes, 17 of which are indecomposable. Six of the codes have minimum weight 6.

I. Self-Orthogonal Ternary Codes of Minimum Weight 6

A. Introduction

LET C be a self-orthogonal ternary code of length n, dimension k, and minimum weight d: we shall refer to C as an $[n,k,d]$ code. It is often convenient to regard C as consisting of a number of *components* which are held together by *glue*. This glueing theory has been described in [2] and [3] and will be used in Sections II–IV below. It is most effective when the minimum weight of C is 3. The following theory applies to codes of minimum weight 6.

B. Center Sets

Let us assume then that C is a self-orthogonal code of length n and minimum weight 6. A *hexad* of C is the binary vector of length n which is the support of a pair of codewords $\pm c \in C$ of weight 6. These hexads in fact belong to E_n, the subspace of $GF(2)^n$ consisting of vectors of even weight. The usual inner product on $GF(2)^n$ and E_n will be denoted by $\phi(x,y)$. In particular ϕ is a possibly degenerate symplectic form on E_n ([6, p. 435], [9, p. 2]).

The assumptions about C imply that two distinct hexads of C meet in 0, 2, 3, or 4 coordinates.

Proposition 1: The binary sum of two hexads of C is a hexad of C if and only if the two hexads meet in three coordinates.

The proof is immediate. This implies that the hexads of C form what is called a center set.

Definition: Let V be a finite dimensional vector space over GF(2) equipped with a symplectic form ψ. A nonempty subset J of V is called a *center set* if it has the property that

if x and y are in J, then $x+y$ is in J
if and only if $\psi(x,y)=1$.

Proposition 1 implies the following theorem.

Theorem 2: If C is a self-orthogonal ternary code of length n and minimum weight 6, the hexads of C form a center set in E_n.

The full theory of center sets will be published separately [12]. Here we shall just state the results we need for the coding applications and refer the reader to [12] for proofs.

Associated with any center set J are an undirected graph Γ and a linear group L. The vertices of Γ are identified with the elements of J, and two vertices x and y are joined by an edge if and only if $\psi(x,y)=1$. The group L is the group of linear transformations on V generated by the mappings

$$t_x: y \rightarrow y+\psi(x,y)x, \qquad y \in V,$$

for $x \in J$. The mapping t_x is called a *transvection with center* x ([5, p. 10], [8]).

Proposition 3 [*12*]*:* The group L carries the set J onto itself, and the orbits of L in J are exactly the connected components of Γ.

If Γ is connected, J is called a *connected* center set. The smallest example is the *trivial* center set, consisting of a single element x in a vector space $V=\langle x\rangle$.

The advantage of this approach is that it is possible to give an explicit description of all the connected center sets. Thus let J be a nontrivial connected center set spanning its vector space V, with associated graph Γ and group L.

Proposition 4 [*12*]*: J* is the entire collection of centers of the nontrivial transvections in L (whence the name "center set" for J).

The *radical* of a symplectic form ψ on V is the subspace

$$\operatorname{rad}\psi=\{x \in V \mid \psi(x,y)=0 \text{ for all } y \in V\}.$$

Manuscript received May 20, 1979; revised July 11, 1979. This work was supported in part by the National Science Foundation under Grants MCS 760-3143 and MCS 78-01458.

V. Pless is with the Mathematics Department, University of Illinois at Chicago Circle, Box 4348, Chicago, IL 60680.

N. J. A. Sloane is with the Mathematics Research Center, Bell Laboratories, Inc., Room 2C-363, Murray Hill, NJ 07974.

H. N. Ward is with the Mathematics Department, University of Virginia, Cabell Hall, Charlottesville, VA 22903.

0018-9448/80/0500-0305$00.75 ©1980 IEEE

Let $\bar{V}=V/\mathrm{rad}\,\psi$, with $\bar{\ }$ the corresponding quotient homomorphism of V onto $\bar{V}$. Thus $\bar{J}$ is the image of J and $\bar{\psi}$ is the form on $\bar{V}$ induced by ψ. Let $\bar{L}$ be the linear group induced on $\bar{V}$ by L. Then $\bar{L}$ has $\bar{J}$ as the set of centers of its transvections.

Proposition 5 [*12*]*:* If J is a connected center set spanning V, then $\bar{L}$ acts irreducibly on $\bar{V}$.

Proposition 5 enables us to apply McLaughlin's classification [8] of the irreducible groups generated by transvections and to obtain the following result.

Theorem 6: If J is a connected center set spanning V, then $\bar{L}$ is one of the following groups:

1) the symplectic group of the form $\bar{\psi}$;
2) the full orthogonal group of a quadratic form having $\bar{\psi}$ as the corresponding symplectic form;
3) a symmetric group $\mathbb{S}_r$ acting on $\bar{V}$ in one of the representations discovered by L. E. Dickson (see [4] and Section C below).

If case 3) holds, the center set is said to be of *symmetric type*. These are the only ones that occur in the coding applications.

Theorem 7 [*12*]*:* A connected center set which is formed from the hexads of a code as in Theorem 2 is of symmetric type.

C. Connected Center Sets of Symmetric Type

If J is any connected center set (not necessarily of symmetric type) spanning its vector space V, and x is an element of J, let T be the following subset of V:

$$T=\{t\in \mathrm{rad}\,\psi \mid x+t\in J\}.$$

Proposition 8 [*12*]*:* T does not depend on the choice of x and is a subspace of $\mathrm{rad}\,\psi$.

If V (resp. V') is a vector space with symplectic form ψ (resp. ψ'), V is said to be *isometric* to V' if there is a linear map π: $V\to V'$ such that $\psi(u,v)=\psi'(\pi(u),\pi(v))$ for all $u,v\in V$.

We shall now describe all the connected center sets of symmetric type to within isometry. The subspace T is an important ingredient in the description.

As before E_r denotes the even subspace of $\mathrm{GF}(2)^r$. Let $\boldsymbol{e}$ denote the all-ones vector in E_r and let P_r be the set of $\binom{r}{2}$ pairs, or vectors of weight 2, in E_r. If r is even let E_r' be the quotient $E_r/\langle \boldsymbol{e}\rangle$, and P_r' the image of P_r in the quotient. E_r and E_r' carry the usual inner product ϕ. In E_r, $\mathrm{rad}\,\phi=0$ if r is odd, $\mathrm{rad}\,\phi=\langle \boldsymbol{e}\rangle$ if r is even; while in E_r', $\mathrm{rad}\,\phi=0$. Finally let R_m be any vector space over GF(2) of dimension $m\geq 0$ equipped with the zero form.

Theorem 9 [*12*]*:* Suppose J is a nontrivial connected center set of symmetric type, spanning its vector space V. Then V and J are isometric to exactly one of the following four types:

i) $V=E_r\perp R_m$, with r odd, $r\geq 3$, m arbitrary; ψ agrees with ϕ on E_r; $\mathrm{rad}\,\psi=R_m$; $J=\{\boldsymbol{p}+\rho \mid \boldsymbol{p}\in P_r, \rho\in R_m\}$; and $T=R_m$.

ii) $V=E_r\perp R_m$, with r even, $r\geq 6$, m arbitrary; ψ agrees with ϕ on E_r; $\mathrm{rad}\,\psi=\langle \boldsymbol{e}\rangle+R_m$; $J=\{\boldsymbol{p}+\rho \mid \boldsymbol{p}\in P_r, \rho\in R_m\}$; and $T=R_m$.

iii) $V=E_r\perp R_m$, with r even, $r\geq 8$, m arbitrary; ψ agrees with ϕ on E_r; $\mathrm{rad}\,\psi=\langle \boldsymbol{e}\rangle+R_m$; $J=\{\boldsymbol{p}+\rho, \boldsymbol{p}+\boldsymbol{e}+\rho \mid \boldsymbol{p}\in P_r, \rho\in R_m\}$; and $T=\langle \boldsymbol{e}\rangle+R_m$.

iv) $V=E_r'$, r even, $r\geq 8$; $\psi=\phi$; $\mathrm{rad}\,\psi=0$; $J=P_r'$; and $T=0$.

Let Γ be the graph associated with any of the center sets in Theorem 9. Then we see that in all cases the number of vertices v is given by

$$v=|J|=\binom{r}{2}|T|,$$

and that the graph is regular with valency

$$k=(2r-4)|T|,$$

where $|T|=2^m$, 2^m, 2^{m+1}, or 1 in the four cases. We denote this graph by C_k^v, and the graph of the trivial center set by C_0^1. Since

$$\frac{4v}{k}=r+1+\frac{2}{r-2},$$

the numbers v and k determine r and hence $|T|$. The first few values of the parameters (those for which the valency is ≤ 24) are shown in Table I.

We also see from Theorem 9 that in all cases the graph C_k^v can be constructed as follows (see Fig. 1). First construct the triangular graph $T(r)$ whose $\binom{r}{2}$ vertices correspond to the pairs in an r-set, two pairs being joined by an edge if and only if they meet. Then replace each vertex by $|T|$ disconnected vertices, vertices in different replacements being connected exactly when the original ones were.

Finally we note that in all cases $\bar{V}=E_r/\mathrm{rad}\,\phi$, $\bar{J}=$ image of P_r under $\bar{\ }$, and $\bar{L}$ acting on $\bar{J}$ is isomorphic to the symmetric group $\mathbb{S}_r$.

D. Examples

a) The [9,2,6] code with generator matrix

$$\begin{array}{r}\boldsymbol{u}:\\ \boldsymbol{v}:\end{array}\begin{bmatrix}111 & 111 & 000\\ 000 & 111 & 111\end{bmatrix}$$

contains six vectors of weight 6: $\pm\boldsymbol{u}$, $\pm\boldsymbol{v}$, $\pm(\boldsymbol{u}-\boldsymbol{v})$. The three hexads corresponding to these vectors are

```
111  111  000
000  111  111
111  000  111
```

and form a connected center set J of size 3. The corresponding hexad graph $\Gamma=C_2^3$ is a triangle.

b) The [10,4,6] Golay code g_{10} (see Section III) contains 30 hexads. These form two connected components of size 15, and the graph Γ is $2C_8^{15}$.

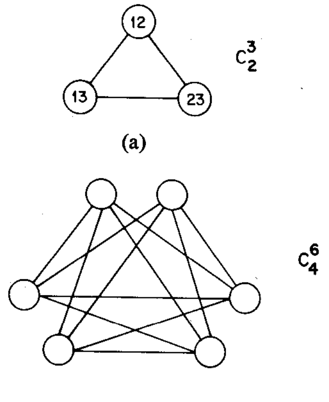
Other examples will be found in Sections III and IV.

TABLE I
PARAMETERS OF NONTRIVIAL CONNECTED CENTER SETS J OF SYMMETRIC TYPE (SEE THEOREM 9)

v:	3	6	10	12	15	20	21	24	28	30	36	40	42
k:	2	4	6	8	8	12	10	16	12	16	14	24	20
r:	3	3	5	3	6	5	7	3	8	6	9	5	7
|T|:	1	2	1	4	1	2	1	8	1	2	1	4	2
type:	i	i	i	i	ii	i	i	i	ii,iv	ii	i	i	i

v:	45	55	56	66	78	91
k:	16	18	24	20	22	24
r:	10	11	8	12	13	14
|T|:	1	1	2	1	1	1
type:	ii,iv	i	ii,iii	ii,iv	i	ii,iv

$v=|J|$ is the number of vertices, and k is the valency of the associated graph $\Gamma = C_k^v$.



(a)

(b)

Fig. 1. Examples of graphs Γ corresponding to connected center sets. (a) $C_2^3 = T(2)$. (b) C_4^6, obtained by replacing each vertex of C_2^3 by two disconnected vertices.

II. CLASSIFICATION OF SELF-DUAL CODES OF LENGTH 20

Encouraged by the application of self-dual codes in a recent attack on the projective plane of order ten [1], we have extended the classification of ternary self-dual codes that was begun in [7] and [3] (see also [11]) to length 20. The result is as follows.

Theorem 10: There are 24 inequivalent ternary self-dual codes of length 20. Of these 7 are decomposable (given in Table II) and 17 are indecomposable (given in Table III). The smallest group of any of these codes has order 512 (code #20), while the largest has order $2^{23}\cdot 3^6\cdot 5$ (code #1). Table IV gives the number of inequivalent maximal self-orthogonal codes of lengths 17, 18, and 19 that can be obtained by contracting each of the codes of length 20 (cf. [3, Section VI]).

We shall use the vocabulary and notation of [3]. Only a sketch of the proof will be given. Enough information will be given about the codes, however, to make it possible for the reader to verify the theorem by checking the group orders of the codes in Tables II and III. There are

$$\prod_{i=0}^{9}(3^i+1) = 9246374028206585446400$$

distinct codes of length 20, which must be sorted into equivalence classes to prove the theorem. The decomposable codes and the indecomposable codes with at least four vectors of weight 3 can be dealt with by the method of glueing: these codes are described in Section III. For the codes with either two or zero vectors of weight 3 we have made extensive use of the theory of center sets given in Section I: these codes are described in Section IV.

The Tables only give A_3, the number of codewords of weight 3, but the full weight distribution is then given by

$$\begin{aligned} A_6 &= 120+13A_3,\\ A_9 &= 4360+19A_3,\\ A_{12} &= 26280-145A_3,\\ A_{15} &= 25728+176A_3,\\ A_{18} &= 2560-64A_3. \end{aligned} \tag{1}$$

As in [2] and [3], $G(C)$ denotes the group of all monomial transformations preserving the code C. $G(C)$ is decomposed into $G_2(C)$ (permuting the components), $G_1(C)$ (fixing the components but permuting the glue vectors modulo the components), and $G_0(C)$ (fixing the components and the glue vectors modulo the components). The orders of these groups are $g(C)$, $g_2(C)$, $g_1(C)$, and $g_0(C)$, respectively, and $g(C)=g_0(C)g_1(C)g_2(C)$.

An essential tool for determining these groups was a computer program which found the distribution of the overlaps among the hexads of a code, and the connected components of the hexad graph Γ (see Section I-B). Whenever a code is decomposed into components or blocks (as shown for example by the Roman numerals in Fig. 9), it is implied that this decomposition is well-defined, in other words is preserved by the group of the code. This decomposition was usually established by studying the output from the above computer program.

We also found it helpful to consider the sums

$$T_i = \sum_{C\in\Omega_i}\frac{1}{g(C)},$$

where Ω_i is the class of inequivalent ternary self-dual codes of length 20 containing exactly $2i$ words of weight 3. These numbers may be calculated directly (without knowing the codes), as in Theorem 2 of [3]. In particular

$$T_0 = \frac{4049}{2^{11}\cdot 3^3\cdot 5^2},$$

$$T_1 = \frac{1}{2^6\cdot 3^3},$$

$$T_2 = \frac{209}{2^8\cdot 3^5\cdot 5\cdot 7}.$$

TABLE II
SELF-DUAL TERNARY CODES OF LENGTH 20
(a) DECOMPOSABLE CODES

#	Components	A_3	g_0	g_1	g_2	glue
1	$5e_4$	40	48^5	1	5!	-
2	$4e_3+2e_4$	24	$6^4\cdot 48^2$	2	$2\cdot 4!$	$\underset{\sim}{aaa000}$, $\underset{\sim}{0a\bar{a}a00}$.
3	$g_{12}+2e_4$	16	$190080\cdot 48^2$	1	2!	-
4	$4e_3+f_4+e_4$	16	$6^4\cdot 1\cdot 48$	8	4!	$(\underset{\sim}{a000})(2111)\underset{\sim}{0}$.
5	$2e_3+g_{10}+e_4$	12	$6^2\cdot 360\cdot 48$	4	2!	$\underset{\sim}{a0x0}$, $\underset{\sim}{0ay0}$.
6	$e_3+p_{13}+e_4$	10	$6\cdot 5616\cdot 48$	2	1	$\underset{\sim}{a}t_0\underset{\sim}{0}$.
7	$h_{16}+e_4$	8	$(2^8\cdot 168)\cdot 48$	1	1	-

TABLE III
SELF-DUAL TERNARY CODES OF LENGTH 20
(b) INDECOMPOSABLE CODES

#	Components	A_3	g_0	g_1	g_2	glue
8	$6e_3+f_2$	12	$6^6\cdot 1$	4	$2\cdot 6^2$	$\underset{\sim}{aaa000}$ 00, $\underset{\sim}{000aaa}$ 00, $\underset{\sim}{0a\bar{a}000}$ 11, $\underset{\sim}{0000a\bar{a}}$ 12.
9	$5e_3+f_5$	10	$6^5\cdot 1$	2	5!	$(\underset{\sim}{0aaaa})(10000)$.
10	$4e_3+g_8$	8	$6^4\cdot 1$	2^5	8	$\underset{\sim}{aa00}$ 1000 2000, $\underset{\sim}{a\bar{a}00}$ 0100 0200, $\underset{\sim}{00aa}$ 0010 0020, $\underset{\sim}{00a\bar{a}}$ 0001 0002.
11	$3e_3+g_{11}$	6	$6^3\cdot 7920$	2	3!	$\underset{\sim}{aaa0}$, $\underset{\sim}{0a\bar{a}u}$.
12	$3e_3+\gamma_{11}$	6	$6^3\cdot(3!)^2$	2^2	2	$\underset{\sim}{a00r}$, $\underset{\sim}{0a0s}$, $\underset{\sim}{0aat}$.
13	$2e_3+g_{10}+f_4$	4	$6^2\cdot 360\cdot 1$	2^4	2	$\underset{\sim}{00x}$ 1200, $\underset{\sim}{00y}$ 0012, $\underset{\sim}{a00}$ 1111, $\underset{\sim}{0a0}$ 2211.
14	$2e_3+p_{12}+f_2$	4	$6^2\cdot 432\cdot 1$	2	2	$\underset{\sim}{00t'_0}$ 12, $\underset{\sim}{a0t'_3}$ 01, $\underset{\sim}{aa0}$ 11.
15	$2e_3+h_{14}$	4	$6^2\cdot 96$	4	2	$\underset{\sim}{a0x}$, $\underset{\sim}{0ay}$.
16	$2e_3+\eta_{14}$	4	$6^2\cdot 84$	4	2	$\underset{\sim}{a0x}$, $\underset{\sim}{0ay}$.
17	$e_3+f_8+2f_4+f_1$	2	$6\cdot 1^4$	$2^7\cdot 3$	1	See Figure 4.
18	$e_3+g_9+g_8$	2	$6\cdot 1\cdot 1$	$2^7\cdot 3^2$	1	See Figure 5.
19	$10f_2$	0	1	2^5	5!	See Figure 7.
20	$4f_4+2f_2$	0	1	2^7	4	See Figure 8.
21	$5f_4$	0	1	2^{10}	10	See Figure 9.
22	$4f_5$	0	1	$2\cdot 5!$	8	See Figure 10.
23	$2g_9+f_2$	0	1	$2^6\cdot 3^4$	2	See Figure 11.
24	$2g_{10}$	0	360^2	2^3	2	$\underset{\sim}{x}$ $\underset{\sim}{x}+\underset{\sim}{y}$, $-\underset{\sim}{x}+\underset{\sim}{y}$ $\underset{\sim}{x}$.

TABLE IV
THE NUMBER OF MAXIMAL SELF-ORTHOGONAL CODES OF LENGTH 17, 18, 19

Parent Code	Number of Children of Length		
of Length 20	17	18	19
1	1	2	1
2	2	5	2
3	1	4	2
4	2	7	3
5	2	7	3
6	2	6	3
7	1	4	2
8	1	4	2
9	1	4	2
10	1	6	2
11	1	4	2
12	2	13	4
13	1	8	3
14	1	7	3
15	1	9	3
16	1	6	2
17	1	16	5
18	1	12	4
19	0	4	1
20	0	5	1
21	0	3	1
22	0	10	1
23	0	6	1
24	0	2	1

These numbers provided intermediate checks on the calculations. For example, summing $g(C)^{-1}$ for codes #19 through #24, we have (see Table III)

$$\frac{1}{2^5\cdot 5!}+\frac{1}{2^7\cdot 4}+\frac{1}{2^9\cdot 10}+\frac{1}{2\cdot 5!\cdot 8}+\frac{1}{2^6\cdot 3^4\cdot 2}+\frac{1}{360^2\cdot 2^3\cdot 2}=\frac{4049}{2^{11}\cdot 3^3\cdot 5^2}=T_0,$$

verifying that these are all the codes of minimum weight 6. A direct proof of this fact is given in Section IV.

Finally we mention two corrections to [7]. In Table 1, p. 659, the order of the group of the Golay code g_{11} (there called G_{11}) is given incorrectly: it should be $2^5\cdot 3^2\cdot 5\cdot 11$. In the penultimate line of that table the code $4C_3(12)$ should carry an asterisk, since it is indecomposable.

III. CODES OF LENGTH 20 WITH $A_3 \geq 4$

The decomposable codes (see Table II) and the indecomposable codes with $A_3 \geq 4$ (#8–16 of Table III) are efficiently described as being made up of various components held together by glue vectors. We first list the components and then supply some additional notes on codes #8, 10, 12, and 13.

In describing the glue vectors in the Tables, an overbar indicates the negative of a vector.

	1	2	3	4	5	6	7	8	9	10	11
γ_{11}	1	1	1	1	1	1	0	0	0	0	0
	1	1	1	0	0	0	1	1	1	0	0
	1	2	0	1	2	0	1	2	0	0	0
	0	0	0	1	2	0	2	1	0	1	2

r	1	1	0	0	0	1	0	0	1	0	0
s	1	0	0	2	0	0	0	0	2	1	0
t	0	0	0	0	0	0	0	0	0	1	1

u	1	1	1	1	1	1	0	0	0	0	0
v	1	1	1	0	0	0	1	1	1	0	0
w	0	0	0	1	1	1	2	2	2	0	0
x	1	2	0	1	2	0	1	2	0	0	0
y	0	1	2	2	0	1	2	0	1	0	0
z	1	0	2	0	2	1	0	2	1	0	0

Fig. 2. The [11,4,6] code γ_{11}, generators $\boldsymbol{r}$, $\boldsymbol{s}$, $\boldsymbol{t}$ for its glue, and six special codewords of weight 6 in γ_{11}. (The vertical lines separating coordinates 3 and 4, and 6 and 7 are drawn only for convenience: this division of coordinates is not preserved by the group. Similar remarks apply to Figs. 2, 4, and 10).

A. The Component Codes (see also [3]*)*

The code e_3 is a [3,1,3] code with generator matrix (111). The glue words are $\pm \boldsymbol{a}$, where $\boldsymbol{a}=120$. Also $g_0=6, g_1=2$.

The code e_4 is a [4,2,3] self-dual code with generator matrix

$$\begin{bmatrix} 1110 \\ 0121 \end{bmatrix}$$

and has no glue. Also $g_0=2|\mathfrak{S}_4|$, $g_1=1$.

The code f_n is the free (or empty) code, indicating a block of n independent coordinates.

The code g_{12} is the [12,6,6] self-dual Golay code. There is no glue. Also $g_0=2|\mathcal{M}_{12}|=2^7\cdot 3^3\cdot 5\cdot 11=190080$, $g_1=1$, and $A_6=2\cdot 132$. There are 132 hexads, and the hexad graph Γ consists of a single connected component C_{40}^{132} (see Section I).

The code g_{11} is the [11,5,6] code consisting of the vectors $\boldsymbol{c}$ such that $0\boldsymbol{c}\in g_{12}$. If a vector $\boldsymbol{u}$ of weight 5 is chosen so that $1\boldsymbol{u}\in g_{12}$ then the glue words for g_{11} may be taken to be $\pm \boldsymbol{u}$. Also $g_0=|\mathcal{M}_{11}|=2^4\cdot 3^2\cdot 5\cdot 11=7920$, $g_1=2$, $A_6=2\cdot 66$, $\Gamma=C_{20}^{66}$.

The code γ_{11} is the [11,4,6] code with generator matrix shown in Fig. 2. The figure also shows generators $\boldsymbol{r}$, $\boldsymbol{s}$, and $\boldsymbol{t}$ for the glue. For this code $A_6=2\cdot 21$ and $\Gamma=2C_2^3+C_8^{15}$. Let us denote the hexads forming the two C_2^3 components by $\{\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}\}$ and $\{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\}$ respectively. Codewords corresponding to these hexads are shown in Fig. 2. The group $G_0(\gamma_{11})$ contains

$$\pi_1=(4,7)(5,8)(6,9)(10,11),$$

producing the permutation $(\boldsymbol{u},\boldsymbol{v})$ on the hexads,

$$\pi_2=(1,8)(2,7)(3,9)(10,11)\,\mathrm{diag}\{2^3\ 1^3\ 2^3\ 1^2\},$$

producing $(\boldsymbol{u},\boldsymbol{w})$; and $G_1(\gamma_{11})$ contains $-I$,

$$\pi_3=(1,4)(3,7)(6,8)\,\mathrm{diag}\{121^2\ 2^2\ 1\ 2^4\},$$

$$\begin{array}{c|ccc|ccc|ccc|}
 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline
 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
g_9 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 \\ \hline
\end{array}$$

$$\begin{array}{c|ccc|ccc|ccc|}
\hline
r & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
s & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\
t & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\ \hline
\end{array}$$

Fig. 3. The [9,3,6] code g_9 and generators $\boldsymbol{r}$, $\boldsymbol{s}$, $\boldsymbol{t}$ for its glue.

producing $(\boldsymbol{u},\boldsymbol{x})(\boldsymbol{v},\boldsymbol{y})(\boldsymbol{w},\boldsymbol{z})$ on the hexads, and

$$\pi_4=(10,11)\operatorname{diag}\{1^9\ 2^2\}.$$

Thus $g_0=(3!)^2$, $g_1=2^3$, $g=2^5\cdot 3^2=288$.

The code g_{10} is the [10,4,6] code consisting of the vectors $\boldsymbol{c}$ such that $00\boldsymbol{c}\in g_{12}$. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are chosen so that $11\boldsymbol{x}\in g_{12}$, $12\boldsymbol{y}\in g_{12}$, then the glue words for g_{10} may be taken to be

$$\begin{array}{ll}
\pm\boldsymbol{x} & \text{of weight 4,} \\
\pm\boldsymbol{y} & \text{of weight 4,} \\
\pm(\boldsymbol{x}+\boldsymbol{y}) & \text{of weight 5,} \\
\pm(\boldsymbol{x}-\boldsymbol{y}) & \text{of weight 5.}
\end{array} \tag{2}$$

Also $g_0=2^3\cdot 3^2\cdot 5=360$, $g_1=2^3$ (generated by $-I$, $(\boldsymbol{x},\boldsymbol{y})$, and $(\boldsymbol{y},-\boldsymbol{y})$), $A_6=2\cdot 30$, $\Gamma=2C_8^{15}$.

The code g_9 is the [9,3,6] code with generator matrix shown in Fig. 3. The figure also shows generators $\boldsymbol{r}$, $\boldsymbol{s}$, and $\boldsymbol{t}$ for the glue. For this code $g_0=1$, $g_1=2\cdot 9\cdot 8\cdot 6=864$, $A_6=2\cdot 12$, $\Gamma=4C_2^3$.

The code g_8 is the [8,2,6] code with generator matrix

$$\begin{bmatrix} 1110 & 1110 \\ 0121 & 0121 \end{bmatrix},$$

and may be formed by doubling each codeword of e_4. There are four dimensions of glue. Also $g_0=1$, $g_1=2^8\cdot 3$, $A_6=2\cdot 4$, $\Gamma=4C_0^1$.

The codes g_{11}, γ_{11}, g_{10}, g_9, and g_8 are all subcodes of g_{12}.

The code p_{13} is a [13,6,6] code described in Section VI of [3]. It is dual to the [13,7,4] code generated by the lines $\boldsymbol{t}_0,\boldsymbol{t}_1,\cdots,\boldsymbol{t}_{12}$ of the projective plane of order 3. We label the points of the plane $Q_0,\cdots,Q_{12}$, and take t_i to be the ith cyclic shift to the right of the line

$$\boldsymbol{t}_0=\begin{pmatrix} Q_0 & Q_1 & Q_2 & Q_3 & Q_4 & Q_5 & Q_6 & Q_7 & Q_8 & Q_9 & Q_{10} & Q_{11} & Q_{12} \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then p_{13} consists of the vectors $\Sigma a_i t_i$ with $\Sigma a_i=0$. The glue words for p_{13} are $\pm\boldsymbol{t}_0$. Also $g_0=|\mathrm{PGL}_3(3)|=2^4\cdot 3^3\cdot 13=5616$, $g_1=2$, $A_6=2\cdot 78$, $\Gamma=C_{22}^{78}$.

The code p_{12} is the [12,5,6] code consisting of the vectors $\boldsymbol{c}$ such that $\boldsymbol{c}0\in p_{13}$, i.e. which vanish at the point Q_{12}. The glue words for p_{12} may be taken to be

$$\begin{array}{ll}
\pm t_0' & \text{of weight 4,} \\
\pm t_3' & \text{of weight 3,} \\
\pm(t_0'-t_3') & \text{of weight 5,} \\
\pm(t_0'+t_3') & \text{of weight 6,}
\end{array} \tag{3}$$

where the primes indicate that the last coordinate is deleted. Also $g_0=432$, $g_1=2$, $A_6=2\cdot 42$, $\Gamma=C_{14}^{36}+C_4^6$.

The code h_{16} is the unique [16,8,6] self-dual code. It has generator matrix $[I_8 \mid H_8]$, where H_8 is an 8×8 Hadamard matrix. There is no glue, and $g_0=2^8\cdot 168=2^{11}\cdot 3\cdot 7=43008$, $g_1=1$, $A_6=2\cdot 112$, $\Gamma=2C_{24}^{56}$. (This code was denoted by $2f_8$ in [3], but it is now convenient to regard it as a component in its own right. This renaming changes the values of g_0, g_1, and g_2, but not of course of g itself.)

The code h_{15} is the [15,7,6] code consisting of the vectors $\boldsymbol{c}$ such that $0\boldsymbol{c}\in h_{16}$. If a vector $\boldsymbol{u}$ of weight 5 is chosen so that $1\boldsymbol{u}\in h_{16}$, then the glue words for h_{15} may be taken to be $\pm\boldsymbol{u}$. Also $g_0=2^6\cdot 3\cdot 7=1344$, $g_1=2$, $A_6=2\cdot 70$, $\Gamma=C_{20}^{42}+C_{12}^{28}$.

The code h_{14} is the [14,6,6] code obtained by deleting two coordinates from the *same side* of h_{16}. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are chosen so that $11\boldsymbol{x}\in h_{16}$ and $12\boldsymbol{y}\in h_{16}$ then the glue words for h_{14} are given by (2). Also $g_0=96$, $g_1=8$ (as for g_{10}), $g=2^8\cdot 3=768$, $A_6=2\cdot 42$, $\Gamma=C_{16}^{30}+2C_4^6$.

The code η_{14} is the [14,6,6] code obtained by deleting one coordinate from *each side* of h_{16}. The glue words are formally the same as for g_{10} and h_{14}. Also $g_0=84$, $g_1=8$, $g=2^5\cdot 3\cdot 7=672$, $A_6=2\cdot 42$, $\Gamma=2C_{10}^{21}$.

B. The Groups of Codes #8, 10, 12, and 13

Code #8: G_2 contains an $\mathbb{S}_3$ on the first three e_3 and on the second three e_3, and the two sets of three may be exchanged. Thus $g_2=2\cdot 6^2$. Then G_1 is generated by $-I$ and $(19,20)\operatorname{diag}\{1^9\ 2^9\ 1^2\}$, so that $g_1=4$.

Code #10: G_2 contains monomials which accomplish the permutations (I,II) and (I,III)(II,IV) on the e_3 components. Then G_1 is generated by $-I$ and by

$$\begin{array}{l}
(13,14)(17,18)(15,19)\operatorname{diag}\{2^3\ 1^9,\ 2^3\ 1\ 2^3\ 1\}, \\
(13,14)(17,18)(16,20)\operatorname{diag}\{1^3\ 2^3\ 1^6,\ 1^3\ 2\ 1^3\ 2\}, \\
(15,16)(19,20)(13,17)\operatorname{diag}\{1^6\ 2^3\ 1^3,\ 212^3\ 12^2\}, \\
(15,16)(19,20)(14,18)\operatorname{diag}\{1^9\ 2^3,\ 121^3\ 21^2\},
\end{array}$$

each of which multiplies a different e_3 component by 2.

Code #12: G_2 contains (II,III) on the e_3 components. G_1 contains only half of $G_1(\gamma_{11})$, since the element $(10,11)\operatorname{diag}\{1^9\ 2^2\}$ of $G_1(\gamma_{11})$ is missing.

Code #13: G_1 contains $-I$, as well as eight elements which when restricted to the g_{10} component form the full group $G_1(g_{10})$. Thus for code #13 $g_1=2\cdot 2^3$.

IV. Codes of Length 20 with $A_3=0$ or $A_3=2$

A. A Theorem about Glueing

The following result underlies much of glueing theory but does not appear to have been stated explicitly before now. It will be used in the proof of Theorem 12.

Theorem 11: Let C be a self-dual code of length $n=n_a+n_b$ over GF(q). Partition the generator matrix of C as follows:

$$\begin{array}{c|c|c|}
 & n_a & n_b \\ \hline
k_a & A & 0 \\ \hline
k_b & 0 & B \\ \hline
k_d & D & E \\ \hline
\end{array}$$

where k_a and k_b are to be chosen as large as possible. Then

i) $k_d = \operatorname{rank} D = \operatorname{rank} E$,

ii) $k_b = \frac{1}{2}n - (n_a - k_a)$,

iii) the code generated by the rows of A and D is the dual of the code generated by the rows of A.

Proof: i) The assertion is that the rank of E (and D) coincides with the number of rows of E. Suppose on the contrary that there is a nontrivial linear combination of the last k_d rows which has the form $\boldsymbol{u0}$ (with length $(\boldsymbol{u}) = n_a$, length $(\mathbf{0}) = n_b$). But then $\boldsymbol{u}$ is in the code generated by the rows of A (by definition of A), implying a dependency among the rows of the generator matrix, a contradiction.

ii) and iii) Since C is self-dual, the rows of D are orthogonal to the rows of A. Thus

$$k_d + k_a \leqslant n_a - k_a. \tag{4}$$

Similarly

$$k_d + k_b \leqslant n_b - k_b. \tag{5}$$

Therefore

$$k_d + k_a + k_b \leqslant \tfrac{1}{2}(n_a + n_b) = \tfrac{1}{2}n. \tag{6}$$

But since C is self-dual, equality holds in (6) and hence in (4) and (5). Q.E.D.

Remarks: a) Theorem 11 implies that the space of glue vectors of the left (spanned by the rows of D) is isomorphic to the space of glue words on the right (spanned by the rows of E).

b) A special case of the decomposition of C used in the proof of Theorem 11 (when C is the Golay code of length 24, $A = (1^8)$, and B is a $[16,5,8]$ code) is the starting point for one of the constructions of the Nordstrom–Robinson code (cf. [6, p. 73]).

B. Codes of Length 20 and Minimum Weight 6

Theorem 12: If C is a ternary self-dual code of length 20 and minimum weight 6, its hexad graph Γ has 60 vertices and is regular with valency 8.

Proof: From (1), $A_6 = 120$, so C contains 60 hexads. If $\boldsymbol{u}$ is any one of these hexads, each hexad $\boldsymbol{v}$ connected to $\boldsymbol{u}$ comes from a vector of weight 6 projecting onto a vector of weight 3 on the 14 coordinates outside $\boldsymbol{u}$. Let B be the code of length 14 supported on the coordinates outside $\boldsymbol{u}$ and consisting of the vectors of C whose supports miss $\boldsymbol{u}$. By Theorem 11 these projections of weight 3 are exactly the vectors of $B^{\perp}$ of weight 3. Now $B^{\perp}$ has no vectors of weight 1 (since they would project from vectors of weight 6 meeting $\boldsymbol{u}$ in five places); and the weights in B are 0, 6, 9, or 12. B has dimension $10-6+1=5$, by Theorem 11 ii). If we set up the MacWilliams identities connecting $B^{\perp}$ and B, it turns out that these restrictions imply that the number of vectors of weight 3 in $B^{\perp}$ is eight, independent of the weight distribution of B. Thus the valency of the vertex $\boldsymbol{u}$ is eight, as required. Q.E.D.

Using Theorem 12 we may establish the following theorem.

Theorem 13: There are exactly six codes of length 20 and minimum weight 6: these are #19–#24 of Table III.

Sketch of Proof: From Table I we see that there are only two connected graphs with valency 8: C_8^{12} and C_8^{15}. Furthermore there are only two ways these components can be combined to produce a graph with 60 vertices: either by taking four components of type C_8^{15}, or five of type C_8^{12}. Thus $\Gamma = 4C_8^{15}$ or $5C_8^{12}$. In addition, the Assmus–Mattson theorem [6, th. 29, p. 177] shows that the hexads form a 1-design. Thus each coordinate position is covered by $60 \times 6/20 = 18$ hexads.

C. The Codes with $\Gamma = 4C_8^{15}$

We must investigate how the four copies of C_8^{15} can fit together in the code. Each C_8^{15} is isometric to the set of pairs P_6 in the even subspace E_6 of $\mathrm{GF}(2)^6$ (this is case ii) of Theorem 9 with $r=6$, $R_m=0$). Furthermore P_6 spans E_6.

Now let us examine the copies of C_8^{15} regarded as made up of hexads. Let $J_1, \cdots, J_4$ denote the four components, regarded as consisting of binary vectors of length 20 and weight 6, let $E^{(i)}$ be the binary span of J_i, and let W be the binary code of length 20 spanned by the union of $J_1, \cdots, J_4$. The form ϕ on W is the natural inner product, as before. Then each J_i is isometric to P_6, each $E^{(i)}$ is isometric to E_6, and each $E^{(i)}$ contains an element $\boldsymbol{e}^{(i)}$ (say) which corresponds under the isometry to the all-ones vector $\boldsymbol{e}_6$ in E_6. Also $\operatorname{rad}(\phi|E^{(i)}) = \langle \boldsymbol{e}^{(i)} \rangle$, and $\operatorname{rad}\phi = \langle \boldsymbol{e}^{(1)}, \cdots, \boldsymbol{e}^{(4)} \rangle$. Of course some of the $\boldsymbol{e}^{(i)}$ may coincide, and we shall show that there are exactly two distinct $\boldsymbol{e}^{(i)}$'s.

To do this we use a tool helpful in constructing the codes: we consider the coordinate functionals as linear functionals on W and the $E^{(i)}$. A linear functional on E_6 is conveniently represented by taking a word in $\mathrm{GF}(2)^6$ and forming its inner product with the members of E_6. A word and its complement will produce the same functional on E_6, so that the weight of the word may be taken to be 0, 1, 2, or 3. A functional produced by a word of weight w will be called a *w-set functional.* A w-set functional takes the value 1, or *registers,* on $w(6\text{-}w)$ members of P_6, namely those half in and half out of the given word. Thus the possible number of times a functional can register on P_6—the *size* of the functional—is 0, 5, 8, or 9. Since a coordinate functional registers on 18 hexads, the two sums

$$18 = 9+9+0+0 \quad \text{and} \quad 18 = 5+5+8+0$$

represent the only dispositions of sizes of a coordinate functional on the four J_i's. It is the odd-size functionals that register on e_6. That means each coordinate registers on two of the $e^{(i)}$. As no $e^{(i)}$ is 0, there are at least two distinct $e^{(i)}$ and $\dim(\mathrm{rad}\,\phi) \geqslant 2$.

On the other hand, let e_{20} be the all-ones word in $E_{20} \subseteq \mathrm{GF}(2)^{20}$. Let a prime denote the mapping $E_{20} \rightarrow E_{20}/\langle e_{20}\rangle = E'_{20}$. E'_{20} is nonsingular under the inherited symplectic form, and $W' \subseteq ((\mathrm{rad}\,\phi)')^{\perp}$. As $\dim(\mathrm{rad}\,\phi)' \geqslant 1$, $\dim W' \leqslant 17$, and $\dim W \leqslant 18$. But $W/\mathrm{rad}\,\phi$ is the orthogonal direct sum of the images in $W/\mathrm{rad}\,\phi$ of the four $E^{(i)}$, and each image has dimension 4 and is nonsingular. Thus $\dim(W/\mathrm{rad}\,\phi) = 16$. As $\dim(\mathrm{rad}\,\phi) \geqslant 2$, we must have $\dim W = 18$ exactly, $\dim(\mathrm{rad}\,\phi) = 2$, and $e_{20} \in \mathrm{rad}\,\phi$. Since e_6 is the sum of three mutually disjoint pairs, each $e^{(i)}$ is the sum of three mutually orthogonal hexads, so that $\mathrm{wt}(e^{(i)}) \equiv 2 \pmod 4$. That means e_{20} is not one of the $e^{(i)}$, so the $e^{(i)}$ must coincide in pairs and the two different ones sum to e_{20}; they are complements. We shall take $e^{(1)} = e^{(2)}$ and $e^{(3)} = e^{(4)}$.

The next step is to consider how many coordinate functionals of each size there can be. Let $f_i(s)$ be the number of coordinate functionals whose size on $E^{(i)}$ is s, so that

$$\sum_{s=0,5,8,9} f_i(s) = 20 \tag{7}$$

and

$$\mathrm{wt}(e^{(i)}) = f_i(5) + f_i(9) \qquad (1 \leqslant i \leqslant 4). \tag{8}$$

Since $E^{(i)}$ contains 15 hexads, the coordinate functionals register $15 \times 6 = 90$ times on them. Thus

$$90 = 5f_i(5) + 8f_i(8) + 9f_i(9). \tag{9}$$

Furthermore, since $E^{(1)}$ and $E^{(2)}$ have the same radical, if a functional is of odd size on $E^{(1)}$ it must be of odd size on $E^{(2)}$. Thus the only types of functionals that can occur are the following:

	←	$e^{(1)}$	→	←	$e^{(2)}$	→	
Number	$f_3(8)$	$f_4(8)$	$f_1(9)$	$f_1(8)$	$f_2(8)$	$f_3(9)$	
Size on $E^{(1)}$	5	5	9	8	0	0	
Size on $E^{(2)}$	5	5	9	0	8	0	
Size on $E^{(3)}$	8	0	0	5	5	9	
Size on $E^{(4)}$	0	8	0	5	5	9.	(10)

This implies that

$$f_1(5) = f_2(5) = f_3(8) + f_4(8), \tag{11}$$

$$f_1(9) = f_2(9), \tag{12}$$

$$f_3(5) = f_4(5) = f_1(8) + f_2(8), \tag{13}$$

$$f_3(9) = f_4(9). \tag{14}$$

From (9)–(14) we have

$$\begin{aligned} f_1(8) &= f_2(8) = a', \\ f_3(8) &= f_4(8) = a, \\ f_1(9) &= f_2(9) = b, \\ f_3(9) &= f_4(9) = b' \quad \text{(say)}, \end{aligned}$$

and

$$\begin{aligned} 10a + 9b + 8a' &= 90, \\ 10a' + 9b' + 8a &= 90, \\ 2a + b + 2a' + b' &= 20. \end{aligned}$$

In particular $2a + b \equiv 2 \pmod 8$, so from (8) $\mathrm{wt}(e^{(1)}) \equiv 2 \pmod 8$. Similarly $\mathrm{wt}(e^{(3)}) \equiv 2 \pmod 8$. Without loss of generality we may take $\mathrm{wt}(e^{(1)}) = 2$ or 10.

Consider now a fixed component space $E^{(i)}$. If we think of it as a copy of E_6, then given one of the six members of the 6-set underlying E_6, say x, we can sort the w-set functionals on $E^{(i)}$ according to whether x is or is not in the w-set. Let a_w be the total number of coordinate functionals (on $\mathrm{GF}(2)^{20}$) which are w-set functionals on $E^{(i)}$, and let $p_w(x)$ be the number whose w-set contains x.

Now look at the hexads corresponding to the five pairs containing x. The total number of times all the coordinate functionals register on these hexads is $5 \times 6 = 30$. A w-set functional containing x registers $6 - w$ times on the five hexads, and one not containing x registers w times. We thus have

$$\begin{aligned} 30 &= \sum_{w=1}^{3} \{(6-w)p_w(x) + w(a_w - p_w(x))\} \\ &= a_1 + 2a_2 + 3a_3 + 4p_1(x) + 2p_2(x). \end{aligned}$$

Such an equation holds for each of the six members x. For the component space $E^{(1)}$ we have $a_1 = 2a$, $a_2 = a'$, and $a_3 = b$; similar equations hold for the others. Finally, $a_1 = \Sigma_x p_1(x)$ and $2a_2 = \Sigma_x p_2(x)$.

Armed with all this, one can set up the four codes (#20, 22, 23, 24 of Table III) that have the graph $4C_8^{15}$. Only code #23 has $\mathrm{wt}(e^{(1)}) = 2$; the others have $\mathrm{wt}(e^{(1)}) = 10$ and accordingly $a = a'$, $b = b'$. We shall illustrate the procedure for code #20; here $a = 4$ and $b = 2$. Thus $4 = 2p_1(x) + p_2(x)$ for any component space and any x, so that $p_1(x) = 0$, 1, or 2.

We select component space $E^{(1)}$, for example, and think of the six members of the 6-set involved as numbered 1 to 6. A w-set functional will be described by giving the numbers in its w-set, as will a pair corresponding to a hexad. From $8 = \Sigma_x p_1(x)$ we find three possible patterns for the eight 1-set coordinate functionals (up to order and renumbering):

1	1	2	2	3	3	4	4
1	2	3	3	4	4	5	5
1	2	3	4	5	5	6	6.

In the first possibility, $p_1(x) = 2$ implies $p_2(x) = 0$. Thus the four 2-set coordinate functionals would all have to be 56. But then the hexad corresponding to 56 could only have the two 3-set functionals registering on it, and would not be a hexad. So this case is eliminated. The second case is ruled out similarly, as is one of the two possible patterns for the 2-set functionals in the third case. The only possible pattern for the 14 coordinate functionals that register on any of the hexads of $E^{(1)}$ is

1 2 3 4 5 5 6 6 13 14 23 24 125 126

(with a suitable numbering). These (more aesthetically set out, the pairs and triples written vertically) label 14 positions in Fig. 8.

To complete the code we lay out the coordinate functionals for one of the component spaces having the other $e^{(i)}$; we select one having one of its 2-set functionals in the same position as one labeled 5. Call this component $E^{(3)}$ and indicate its 6-set with primes. The hexad corresponding to 56 from $E^{(1)}$ must be orthogonal to all hexads of $E^{(3)}$. The only positions in which it can meet a hexad from $E^{(3)}$ are the 5's and 6's. If, for example, the 2-set functional $1'4'$ is at one of the 5's, the hexad corresponding to $1'5'$ will show $1'3'$ must also be at one of the 5's or 6's. Arguing repeatedly in this way, we find that all the 2-set functionals for $E^{(3)}$ are in the 5 and 6 locations. Correspondingly, at the 2-set functionals for $E^{(1)}$ we must have the 1-set functionals $5'$ and $6'$ for $E^{(3)}$. For if not, suppose $1'$ were one of them. Then some other number r' would not appear. The hexad for $1'r'$ would then meet the hexad for 12 only once (at the $1'$ spot), violating orthogonality. Finally, to settle on the dispositions in Fig. 8 (allowing renumbering) we invoke things like the orthogonality of the hexads for 15 and $1'4'$.

To obtain the basis for the code (which is still hypothetical at this point!) we begin by filling in *ternary* words of weight 6 whose supports are the hexads corresponding to 12, 13, 14, 15, and 16. These can all be filled in with ones, by scaling, since any two of the words overlap in three positions where they must totally agree (or totally disagree). Similarly we fill in words for the hexads $1'2'$, $1'3'$, $1'4'$, $1'5'$, $1'6'$. This time some twos are needed to obtain orthogonality with the first collection of words. These twos are forced once some free scaling choices have been made. The final pattern appears in Fig. 8 (with the pairs corresponding to the ten hexads being used as row labels).

D. *The Codes with* $\Gamma = 5C_8^{12}$

Now the prototype of the component spans is the orthogonal sum $E_3 \perp R_2$, and the center set is the set of sums $\boldsymbol{p}+\rho$ for $\boldsymbol{p} \in E_3$, $\rho \in R_2$ (see Theorem 9). The sizes of linear functionals on $E_3 \perp R_2$ are 6 and 8, those of size 8 being the ones that vanish on R_2. As before, each coordinate functional registers on 18 hexads, but the only way 18 can be a sum of 6's and 8's is

$$18 = 6+6+6+0+0.$$

Thus no coordinate functional has size 8 on any component space, and each coordinate is covered by three components. Since the coordinates register $12 \times 6 = 72$ times on the hexads of a component, $72/6 = 12$ of the coordinate functionals are nonzero on a component space. That is, each component covers 12 coordinate positions.

If we think of a particular component space as a copy of $E_3 \perp R_2$, the members of R_2 will each be sums of two orthogonal hexads and thus have weights 0, 4, 8, or 12. There are two cases: no member of R_2 for any component corresponds to a word of weight 4; or some member does. Each leads to a code (#19 and #21, respectively) and we shall sketch how code #19 (associated with the Petersen graph) arises.

Since for a component space there are three nonzero radical words (the words corresponding to the nonzero members of R_2) supported on 12 positions with weights 8 or 12 in the case at hand, the weights are in fact all 8. As a consequence two hexads in the component that are not connected, differing by a radical word, meet in two positions.

Consider the ternary span S of the words of weight 6 in a component. S is supported on the 12 positions of the component, and covers all 12. With S considered as a code of length 12, $S^{\perp}$ has no words of weight 1. Since S has at least 24 words of weight 6 (two for each hexad), the MacWilliams identities show $\dim S \geqslant 4$. But S is contained in the subcode B (of the whole ternary code C under consideration) of words that are 0 outside the support of S. From Theorem 11, B has dimension 10—8 plus the dimension of the subcode of C that is 0 on the support of S. Since length 8 will support at most two dimensions of orthogonal words of weight 6, $\dim B \leqslant 4$. Thus in fact $S = B$ and $\dim B = 4$. Moreover, the words of weight 6 outside the support of S must be (after scaling and arranging) the following rows and their negatives (on the eight outside positions):

$$\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 2 & 2 & 2 & 2 \\
0 & 0 & 1 & 1 & 2 & 2 & 1 & 1.
\end{array}$$

Because any two of the hexads represented in this pattern meet in four places, they all belong to different components, necessarily the components other than the one being studied. On the other hand, if one has such a pattern of words of weight 6 in the code (covering eight positions) the hexads will be in four different blocks, and the subcode of C that is 0 on these positions will have dimension 4. The MacWilliams identities again imply that the code has at least 24 words of weight 6. But no hexad from such a word can belong to any of the four components represented, since it would have to meet the representing hexad in two or three places. Thus in fact this subcode is the span of the words of weight 6 giving the hexads of the fifth component, and it contains no other words of weight 6.

There are then exactly five such patterns, one for each component (two components cannot occupy the same 12 positions). Consider the patterns for components A and B (using letters as labels). The hexad for component A appearing in the pattern for component B must be disjoint from all the hexads in the pattern for component A, by the discussion above. That means at most two positions of the pattern for component B occur in the one for component A. Since the hexads for component C in the two patterns meet in at least two positions, this means the two patterns share *exactly* two positions. They are then the unique two positions not covered by either component A or component B (but the pattern shows that they are covered by components C, D, and E). Thus the 20 coordinate positions can be taken in groups of two, one group for each pair of components. Furthermore, the hexad from component B in the pattern for component A (for example) will occupy the six positions labeled AC, AD, and AE. This gives a recipe for the 20 hexads occurring in the five patterns, and it has been used in Fig. 7. The row labels indicate the components in which the displayed hexads lie. This completes the sketch of the proof of Theorem 13.

E. Codes of Length 20 with $A_3=2$

Theorem 14: There are exactly two codes of length 20 with $A_3=2$: these are #17 and #18 of Table III.

Outline of Proof: We consider the [17,8,6] subcode which is zero on the support of the words of weight 3. Its dual has ten words of weight 4 and the valency of a hexad is determined in part by whether there are words of weight 4 supported on the hexad. In one case (code #17) the hexad graph for the length 17 code is $C_6^{10}+C_{12}^{20}+C_{12}^{28}$, and in the other (code #18), it is $2C_0^1+2C_{12}^{28}$, having two isolated hexads. In some ways the analysis here is easier because of the presence of the C_{12}^{28} since these have $r=9$ (see Theorem 9), which is larger than the values of r occurring in the codes with $A_3=0$.

F. The Groups of Codes #17 – 24

Code #17 (see Fig. 4): The group $G_1/\pm I$ is transitive on coordinates $\{4,5,\cdots,11\}$, the stabilizer of 4 has orbits $\{4\}$, $\{8\}$, $\{5,6,7,9,10,11\}$, the stabilizer of 4 and 5 has orbits $\{4\}$, $\{5\}$, $\{8\}$, $\{9\}$, $\{6,7,10,11\}$, and the stabilizer of 4, 5, and 6 is the identity. Thus $g_1=2\cdot8\cdot6\cdot4$.

Code #18 (see Fig. 5): The group G_1 is generated by $-I$ and

$$\pi_1=(4,8,6,5,12,9,11,10)(14,19,18,15)(16,20)\cdot\text{negate}\{5,7,9,10,11,16,20\},$$

$$\pi_2=(4,5)(7,8)(10,11)(14,18),$$

$$\pi_3=(13,20)(15,19)(16,17)\text{negate}\{1,2,3,15,19\},$$

$$\pi_4=(13,16)(14,18)(17,20)\cdot\text{negate}\{1,2,3,13,14,16,17,18,20\}.$$

Let H be the subgroup of $G_1/\pm I$ defined by the action on the coordinates $\{4,5,\cdots,12\}$; H is generated by (the restriction of) π_1 and π_2. Then H is doubly transitive on these nine coordinates, and the stabilizer of two points has order 2, so that $|H|=9\cdot8\cdot2$. Finally the action of $G_1/\pm H$ on the coordinates $\{13,14,\cdots,20\}$ is generated by π_3 and π_4, and has order 4. Thus $g_1=2\cdot9\cdot8\cdot2\cdot4=2^7\cdot3^2$.

Code #19: (See Section D and Figs. 6 and 7). The ten blocks are labeled with pairs of letters from $\{A,B,C,D,E\}$ and are in one-to-one correspondence with the nodes of the Petersen graph shown in Fig. 6. The group G_2 is isomorphic to $\mathbb{S}_5$, the group of the Petersen graph. For example it may be generated by the permutations on the blocks induced by (A,B) and (A,B,C,D,E). The group G_1 is generated by $-I$ and

$$\pi_A=(1,2)(3,4)(5,6)(11,12)\text{negate}\{1,2,3,4\},$$

$$\pi_B=(5,6)(7,8)(9,10)(15,16)\text{negate}\{5,6,7,8\},$$

$$\pi_C=(9,10)(11,12)(13,14)(19,20)\text{negate}\{9,10,11,12\},$$

$$\pi_D=(13,14)(15,16)(17,18)(3,4)\text{negate}\{13,14,15,16\},$$

#17. $e_3+f_8+2f_4+f_1$

e_3 ←— f_8 —→ f_4 f_4 f_1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1																	
			1				1								1	2	2	2	
				1				1							2	1	2	2	
					1				1						2	2	1	2	
						1				1					2	2	2	1	
1	2	0	1				2				1								1
1	2	0		1				2				1							1
1	2	0			1				2				1						1
1	2	0				1				2				1					1
1	2	0									1	1	1	1					

Fig. 4. Code #17.

#18. $e_3+g_9+g_8$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1																	
			1	1	1	1	1	1	0	0	0								
			1	1	1	0	0	0	1	1	1								
			1	2	0	1	2	0	1	2	0								
												1	1	1	0	1	1	1	0
												0	1	2	1	0	1	2	1
0	0	0	1	1	1	0	0	0	0	0	0	1	0	2	2	0	0	0	0
0	0	0	1	0	1	1	0	0	1	0	0	0	0	2	0	0	0	1	0
0	0	0	1	0	2	0	0	0	0	1	2	0	2	0	0	0	1	0	0
1	2	0	0	0	0	0	0	0	0	0	0	1	0	0	1	2	0	0	2

Fig. 5. Code #18.

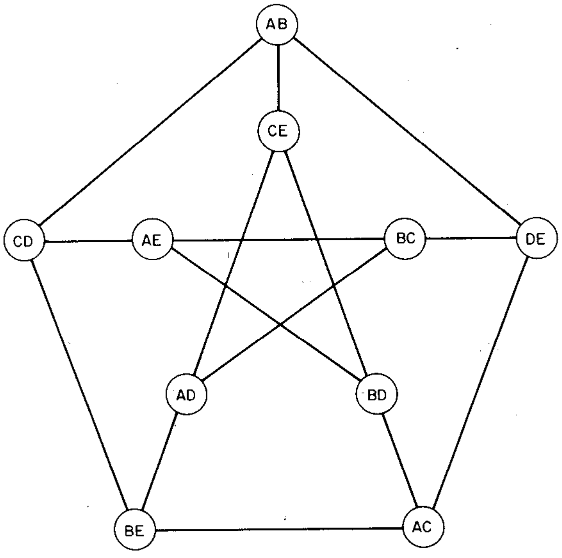


Fig. 6. The Petersen graph, which is the complement of the triangular graph $T(5)$. The nodes are labeled with pairs of letters from $\{A,B,C,D,E\}$, and two nodes are joined by an edge if and only if the corresponding pairs are disjoint. The group of the Petersen graph is $\mathbb{S}_5$, corresponding to all permutations of the five letters.

#19. $10f_2$

	AE		AD		AB		BE		BC		AC		CD		BD		DE		CE	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	1	1	1	1	1	2														
B					1	1	1	1	1	2										
C									1	1	1	1	1	2						
D													1	1	1	1	1	2		
E	1	2															1	1	1	1
A	1	1	2	2							1	2								
B					1	1	2	2							1	2				
C									1	1	2	2							1	2
D			1	2									1	1	2	2				
E							1	2									1	1	2	2

Fig. 7. Code #19.

20. $4f_4+2f_2$

I	II	III	IV	V	VI	
1 2 3 4		5 5 6 6	1 1 2 2 3 4 3 4	1 1 2 2 5 6		FIRST SET OF FUNCTIONALS
	1' 2' 3' 4'	1' 2' 1' 2' 4' 3' 3' 4'	5' 6' 6' 5'		1' 1' 2' 2' 5' 6'	SECOND SET OF FUNCTIONALS
1 1 0 0		0 0 0 0	1 1 1 1	0 0		12
1 0 1 0		0 0 0 0	0 1 1 0	1 1		13
1 0 0 1		0 0 0 0	1 0 0 1	1 1		14
1 0 0 0		1 1 0 0	1 1 0 0	0 1		15
1 0 0 0		0 0 1 1	1 1 0 0	1 0		16
	1 1 0 0	1 2 1 2	0 0 0 0		0 0	1'2'
	1 0 1 0	1 2 0 0	0 0 0 0		1 1	1'3'
	1 0 0 1	0 0 1 2	0 0 0 0		1 1	1'4'
	1 0 0 0	1 0 1 0	2 0 0 1		0 1	1'5'
	1 0 0 0	1 0 1 0	0 2 1 0		1 0	1'6'

Fig. 8. A generator matrix for code #20 is enclosed by the double lines. At the top of the figure are the linear functionals defining the first C_8^{15} component, and below them the linear functionals defining the second C_8^{15}. By evaluating these functionals at the pairs shown on the right, the ten rows of the generator matrix are obtained.

and has order 2^5. These are labeled so that π_i only affects the blocks containing the letter i.

Code #20: (see Section C and Fig. 8). The group G_2 is a Klein group of order 4 acting on the blocks $\{\mathrm{I,II,III,IV}\}$; there is an isomorphic action on the four C_8^{15} components. The group G_1 is best described in terms of the arguments $\{1,2,\cdots,6,1',\cdots,6'\}$ of the linear functionals. It is generated by

$$(1,2)(3,4), \qquad (1,3)(2,4),$$
$$(1',2')(3',4'), \qquad (1',3')(2',4'),$$
$$(3,4)(5',6'), \qquad (5,6)(3',4'),$$

(with suitable signs), and by $-I$, and has order 2^7.

Code #21 (see Fig. 9): G_2 is a dihedral group of order 10 on the blocks, generated by (I, II, III IV, V) and (I, II)(III, IV). G_1 contains $-I$,

$$(1,2)(3,4)(5,6)(7,8)\,\mathrm{diag}\{2^4\ 1^{16}\},$$
$$(3,4)(5,8)(6,7)(11,12)\,\mathrm{diag}\{1^2\ 2^2\ 1^{16}\},$$

and their images under G_2. These generate a group of order 8 on block I, a group of order 8 on block II, and a group of order 8 on the remaining three blocks. Thus $g_1=2\cdot 8^3$.

Code #22 (see Fig. 10): G_2 contains (I, II) and (I, III) (II, IV), and has order 8. G_1 contains $-I$ and an $\mathfrak{S}_5$ on any one block, so $g_1=2\cdot 5!$.

Code #23: The components of this code are $2g_9+f_2$, but in order to determine its group it is better to observe that it contains two copies of γ_{11} having a pair of coordinates (10 and 11 in Fig. 11) in common. G_1 contains

$$\pi_1=(4,7)(5,8)(6,9)(10,11)\,\mathrm{diag}\{1^{18}\ 2^2\},$$
$$\pi_2=(1,8)(2,7)(3,9)(10,11)\,\mathrm{diag}\{2^3\ 1^3\ 2^3\ 1^9\ 2^2\},$$
$$\pi_3=(1,4)(3,7)(6,8)(1',4')(3',7')(6',8')$$
$$\cdot\mathrm{diag}\{1\ 2\ 1^2\ 2^2\ 1\ 2^2,\ 1\ 2\ 1^2\ 2^2\ 1\ 2^2,\ 2^2\},$$

which generate a subgroup H of order 72. When restricted to the coordinates $\{1,\cdots,9,10,11\}$ this subgroup is isomorphic to $G_1(\gamma_{11})/\langle -I,\pi_4\rangle$—see Section III. Nothing else in G_1 (except $-I$) acts on coordinates $\{1,\cdots,9\}$. However G_1 also contains

$$\pi_1'=(4',7')(5',8')(6',9')(10,11)\,\mathrm{diag}\{1^{18}\ 2^2\},$$
$$\pi_2'=(1',8')(2',7')(3',9')(10,11)\,\mathrm{diag}\{1^9\ 2^3\ 1^3\ 2^5\},$$
$$\pi_5'=(1',5')(2',6')(3',4')(7',9')\,\mathrm{diag}\{1^9\ 2^6\ 1^5\},$$
$$\pi_6'=(1',4',8',2',5',7')(3',6',9')(10,11)\,\mathrm{diag}\{1^9\ 2^6\ 1^5\},$$

which generate a group of order 36 on coordinates $\{1',\cdots,9',10,11\}$, isomorphic to a subgroup of H of index 2. Finally G_1 contains $-I$, so that $g_1=2\cdot 72\cdot 36$.

Code #24: G_1 coincides with $G_1(g_{10})$, of order 2^3.

21. $5f_4$

I				II				III				IV				V			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	2	0	0												
				1	1	1	1	1	2	0	0								
								1	1	1	1	1	2	0	0				
												1	1	1	1	1	2	0	0
1	2	0	0													1	1	1	1
2	2	1	1	0	0	1	2												
				2	2	1	1	0	0	1	2								
								2	2	1	1	0	0	1	2				
												2	2	1	1	0	0	1	2
0	0	1	2													2	2	1	1

Fig. 9. Code #21.

22. $4f_5$

I					II					III					IV				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1					1					0	1	1	1	1					
	1					1				1	0	1	1	1					
		1					1			1	1	0	1	1					
			1					1		1	1	1	0	1					
				1					1	1	1	1	1	0					
1					2										0	1	1	1	1
	1					2									1	0	1	1	1
		1					2								1	1	0	1	1
			1					2							1	1	1	0	1
				1					2						1	1	1	1	0

Fig. 10. Code #22.

23. $2g_9+f_2$

1	2	3	4	5	6	7	8	9	1'	2'	3'	4'	5'	6'	7'	8'	9'	10	11
1	1	1	1	1	1	0	0	0											
1	1	1	0	0	0	1	1	1											
1	2	0	1	2	0	1	2	0											
									1	1	1	1	1	1	0	0	0		
									1	1	1	0	0	0	1	1	1		
									1	2	0	1	2	0	1	2	0		
1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0
0	0	1	0	0	2	0	0	2	0	0	2	0	0	1	0	0	1	0	0
0	0	0	1	2	0	2	1	0	0	0	0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	2	1	0	1	2

Fig. 11. Code #23.

Acknowledgment

During the course of this work we have made use of the MACSYMA computer system at the Massachusetts Institute of Technology Laboratory for Computer Science, the CAMAC system at the University of Illinois at Chicago Circle Computer Center, and the Honeywell computer at the Bell Laboratories Murray Hill Computation Center.

References

[1] R. P. Anstee, M. Hall, Jr., and J. G. Thompson, "Planes of order 10 do not have a collineation of order 5," preprint.

[2] J. H. Conway and V. Pless, "On the enumeration of self-dual codes," *J. Combinatorial Theory*, to appear.

[3] J. H. Conway, V. Pless, and N. J. A. Sloane, "Self-dual codes over GF(3) and GF(4) of length not exceeding 16," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 312–322, May 1979.

[4] L. E. Dickson, "Representations of the general symmetric group as linear groups in finite and infinite fields," *Trans. Amer. Math. Soc.*, vol 9, pp. 121–148, 1908.

[5] J. Dieudonné, *Sur les groupes classiques* (Actualités Scientifiques et Industrielles 1040). Paris: Hermann, 1973.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: Elsevier/North Holland, 1977.

[7] C. L. Mallows, V. Pless, and N. J. A. Sloane, "Self-dual codes over GF(3)," *SIAM J. Applied Math.*, vol. 31, pp. 649–666, 1976.

[8] J. McLaughlin, "Some Subgroups of $SL_n(\mathcal{F}_2)$," *Ill. J. Math.*, vol. 13, pp. 108–115, 1969.

[9] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*. New York: Springer–Verlag, 1973.

[10] J. J. Seidel, "Strongly regular graphs," in *Recent Progress in Combinatorics*, W. T. Tutte, Ed. New York: Academic, 1969, pp. 185–197.

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

[12] H. N. Ward, "Center sets and ternary codes," *J. Algebra*, to appear.

A Multiplication-Free Solution for Linear Minimum Mean-Square Estimation and Equalization Using the Branch-and-Bound Principle

TSUN-YEE YAN AND KUNG YAO, MEMBER, IEEE

***Abstract*—An optimal linear mean-square estimation algorithm is derived under the constraint that the algorithm be multiplication-free. A classical linear estimation problem with block length N generally requires N^2 multiplications. For many on-line signal processing situations a large number of multiplications is objectionable. This class of estimation problems includes the classical linear filtering of a random signal in random noise, as well as the linear equalization of digital data over a dispersive channel with additive noise. Here we consider the linear estimation problem on a binary computer where the estimation parameters are constrained to be powers of two and thus all multiplications are replaced by shifts. Then the optimal constrained linear estimation problem resembles an integer-programming problem except that the allowable discrete points are nonintegers. The branch-and-bound principle is used to convert this minimization problem to a series of convex programming problems. An algorithm is given for the solution as well as numerical results for filtering and data equalization. These examples show that the multiplication-free constraint does not generally increase the mean-square error significantly compared with the classical optimal solution. Furthermore, the intuitive "round to the nearest power of two" procedure for the estimation parameters can be inferior to the optimal branch-and-bound solution.**

I. Introduction

RECENT ADVANCES in semiconductor technology have made digital data processing readily available, using either large general purpose scientific computers or special purpose microprocessors. Although micro- and minicomputers are inferior to the big machines both in on-line storage space and operating time, their significantly lower costs have made them extremely attractive in many modern communication, radar, and information-processing systems. Since most of these small machines are relatively slow, good algorithms are particularly important if real-time signal processing is required.

Any algorithm implemented on a computer is contaminated by various kinds of quantization errors caused by the finite word length of the machine [1], [2]. There are the usual analog-to-digital (A/D) quantization errors at the input of the digital system, as well as internal

Manuscript received July 24, 1978; revised May 14, 1979. This work was supported by the Electronics Program of the Office of Naval Research. This paper was presented at the IEEE International Symposium on Information Theory, Grignano, Italy, June 25–29, 1979.

T. Y. Yan was with the Department of System Science, School of Engineering and Applied Science, University of California, Los Angeles. He is now with Xerox Corporation/XTEN, Woodland Hills, CA 91364.

K. Yao is with the Department of System Science, School of Engineering and Applied Science, University of California, Los Angeles, CA 90024.

0018-9448/80/0500-0316$00.75 ©1980 IEEE