JOURNAL OF COMBINATORIAL THEORY, Series A 51, 63–76 (1989)

On Self-Dual, Doubly Even Codes of Length 32

HELMUT KOCH

Karl-Weierstrass-Institut der Akademie der Wissenschaften der DDR, 1080 Berlin, German Democratic Republic

Communicated by Andrew M. Gleason

Received June 15, 1987

We give a new proof for the theorem of Conway and Pless that there are exactly five binary linear self-dual doubly even extremal codes of length 32.

1. INTRODUCTION

In a joint paper [2] Conway and Pless studied binary linear self-dual doubly even codes of length 32 and showed that there are 85 inequivalent such codes (doubly even means that the weights of all code words are multiples of 4). Without doubt the most interesting of them are the five codes of minimal weight 8. These are the extremal codes of type II and length 32 in the terminology of Sloane [4]. We call them CP-codes in the following.

The method of proof in [2] consists in finding codes by several processes "including divination" and then to show by means of the counting formula that one has discovered all the codes. In fact this method is very laborious since one has to compute the automorphism groups of the codes, and if one is only interested in the extremal codes, one has nevertheless to go the long way through all the other 80 codes. In fact, [2] gives only a description of the method of the proof.

In the present paper we give a full and relatively short proof that there are exactly five inequilivalent CP-codes using other methods of proof, which also show something more about the architecture of these codes.

We begin with a description of the five CP-codes. Two of them were known before the investigations of Conway and Pless, namely the extended quadratic residue code for $p = 31$ and the Reed–Muller code $\mathscr{R}(2, 5)$ in the notation of van Lint [3]. We denote these codes here by QR and RM, respectively.

The third CP-code C_3 can be represented in the following form: Let H (resp. H^*) be the extended quadratic residue (resp. non-residue) code for

0097-3165/89 $3.00

582a/51/1-5

$p=7$ such that $H\cap H^*=\{\mathbf{0},\mathbf{1}\}$, where $\mathbf{0}$ (resp. $\mathbf{1}$) denotes the word $(0,\ldots,0)$ (resp. $(1,\ldots,1)$ in $\mathbb{F}_2^8$. Then

$$C_3:=\{(h_1+h_2^*, h_1+h_2+h_2^*, h_2+h_1^*+h_2^*,$$
$$h_2+h_1^*)\,|\,h_1,h_2\in H, h_1^*,h_2^*\in H^*\}.$$

We denote this code by F.

We present the last two codes in the description of Conway and Pless.

Here as in the following we use the set-theoretical notation: Let I be the set of positions of the code. Then a word in $\mathbb{F}_2^I$ considered as a mapping from I to $\mathbb{F}_2$ will be identified with its support. Hence $\mathbb{F}_2^I$ will be identified with the system of subsets of I. Furthermore let $c_1, c_2, \ldots, c_s\in\mathbb{F}_2^I$. Then $(c_1; c_2; \ldots; c_s)$ denotes the set $\{c_i+c_j\,|\,1\leqslant i,j\leqslant s\}$.

For the fourth code of Conway and Pless which will be denoted by U we take $I=\{1,2,\ldots,32\}$. In Table III of [2] this code has the components $8f_4$. This means in our notation that

$$(1,2,3,4;5,6,7,8;\ldots;29,30,31,32)$$

belongs to U. Furthermore, for instance, the word ooyxoxyo in the notation of [2] becomes $\{10,12,15,16,23,24,26,28\}$ in our notation. For the full description of U, we introduce the group Γ generated by the permutation γ:

$$(5,9,13,17,21,25,29)(6,10,14,18,22,26,30)$$
$$\times(7,11,\ldots,31)(8,12,\ldots,32)$$

i.e., γ is a cyclic permutation of the seven tetrads

$$\{5,6,7,8\},\{9,10,11,12\},\ldots,\{29,30,31,32\}.$$

Then U is generated as Γ-module by

$$\{1,2,3,4,5,6,7,8\},\{1,5,9,13,17,21,25,29\},$$
$$\{10,12,15,16,23,24,26,28\},\{3,4,14,16,19,20,22,24\},$$
$$\{6,7,10,12,26,28,30,31\},\{2,4,10,11,18,20,26,27\},$$
$$\{6,7,15,16,23,24,30,31\},\{2,3,7,8,18,19,31,32\}.$$

For the last code Conway and Pless found a nice geometrical description by means of a special basis being invariant under a big subgroup of the automorphism group of the code. Suppose that the 32 positions are arranged as two 4×4 arrays. Then the typical basis element has one non-zero entry in the left array, and 7 in the right, which are precisely those in

the row and column through the element that corresponds to the non-zero entry in the left array. For instance,

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & + & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \qquad \begin{array}{cccc} 0 & + & 0 & 0 \\ + & + & + & + \\ 0 & + & 0 & 0 \\ 0 & + & 0 & 0 \end{array}$$

We denote this code by G.

Our study of CP-codes is based on the following principles:

(a) *The reduction of codes to codes of smaller length* (*Section* 2). Let C be a CP-code which contains a $(15, 4)$-code. Then C can be reduced to the Golay code.

THEOREM 1. *A CP-code which contains a* $(15, 4)$*-code is equivalent to RM, F, or G.*

(b) *The configurations of CP-codes.*

THEOREM 2. *Let a, b, c be arbitrary positions of a CP-code. Then there are exactly seven code words of weight* 8 *containing a, b, c.*

We call the equivalence class in $\mathbb{F}_2^{32}$ of such a set of code words a configuration of the code. The words of a configuration are determined up to equivalence by the positions which appear not less than three times. Each word of the configuration must contain such a position, a pair of such positions can only appear in one word of the configuration, and each word of the configuration can contain no more than three such positions. There are exactly 14 possibilities to arrange positions in seven words with the above conditions. We call them configuration schemes. They are given in Table I. The positions different from a, b, c which appear no less than three times are denoted by d, e, ... The configuration schemes are written in the rows of the table. In the last column of the table one finds the codes which have a configuration given by the configuration scheme of the corresponding row. A bar means that there is no such code.

Theorem 2 is a special case of the theorem of Assmus and Mattson (see, e.g., [1, Theorem 12.13]).

(c) *Verification of the table* (*Section* 3). From our description of the CP-code it is easy to see that the codes QR, RM, F, and G have only the configurations given in the table. In particular, for QR and RM it is well known that their automorphism groups transform each set of three positions in an arbitrary set of three positions so that they have a unique configuration. For U it is not difficult to show that the code has the three

TABLE I

1	*d*	*d*	*d*	*d*	*d*	*d*	*d*	RM, F, U
2	*de*	*d*	*d*	*d*	*d*	*e*	*e*	G, U
3	*de*	*d*	*d*	*d*	*e*	*e*	*e*	G
4	*d*	*d*	*d*	*d*	*e*	*e*	*e*	—
5	*de*	*df*	*d*	*d*	*ef*	*e*	*f*	—
6	*de*	*df*	*dg*	*d*	*ef*	*eg*	*fg*	QR, G
7	*de*	*df*	*d*	*e*	*e*	*f*	*f*	—
8	*def*	*d*	*d*	*e*	*e*	*f*	*f*	G
9	*df*	*dg*	*d*	*ef*	*eg*	*e*	*fg*	—
10	*def*	*dg*	*d*	*eg*	*e*	*fg*	*f*	—
11	*def*	*dg*	*dh*	*eg*	*eh*	*fg*	*fh*	—
12	*def*	*dgh*	*d*	*eg*	*eh*	*fg*	*fh*	—
13	*def*	*dgh*	*di*	*egi*	*eh*	*fg*	*fhi*	U
14	*def*	*dgh*	*dij*	*egi*	*ehj*	*fgj*	*fhi*	F, G

configurations of the table. That it has no other configuration follows from the verification that there are no other CP-codes beside the five codes given above. This is done by means of Theorem 1, Theorem 2, and the following theorem:

THEOREM 3. *Let c be a code word of weight* 16 *of a CP-code C. Then the number of code words of weight* 8 *with support in* supp c *is equal to the number of code words of weight* 8 *with support* in $\operatorname{supp}(\mathbf{1}-c)$.

Theorem 3 is a special case of the balance principle:

Let $C \subset \mathbb{F}_2^n$ be a self-dual linear code and a_1 an arbitrary word in $\mathbb{F}_2^n$. We put $a_2 := \mathbf{1} + a_1$ and $C(a_1) := \{c \in C \mid c \subset a_1\}$. Then

$$|a_1|/2 - \dim C(a_1) = |a_2|/2 - \dim C(a_2). \tag{1}$$

Proof of the balance principle: Let $\langle x_1, x_2 \rangle$ be the standard bilinear form in $\mathbb{F}_2^n$ and $C(a_1)^\perp := \{x \in \mathbb{F}_2^n \mid x \subset a_1,\ \langle x, c \rangle = 0 \text{ for all } c \in C(a_1)\}$. Furthermore let Pr_1 be the linear map from C into $\mathbb{F}_2^{a_1}$ defined by $\mathrm{Pr}_1(c) = a_1 \cap c$ for $c \in C$. It is easy to see that Pr_1 maps into $C(a_1)^\perp$. Therefore we have an exact sequence

$$\{0\} \longrightarrow C(a_2) \longrightarrow C \xrightarrow[\mathrm{Pr}_1]{} C(a_1)^\perp. \tag{2}$$

(2) implies $\dim C(a_2) + \dim C(a_1)^\perp \geqslant \dim C = (|a_1| + |a_2|)/2$, hence

$$|a_1|/2 - \dim C(a_1) \geqslant |a_2|/2 - \dim C(a_2).$$

Changing the roles of a_1 and a_2, we get (1). ∎

2. The Reduction of CP-Codes to Codes of Smaller Length

In this section we are going to prove Theorem 1 by means of reduction of CP-codes to codes of length 24. We need some preparations.

(a) The reduction of CP-codes to codes of smaller length is a special case of a general procedure for the modification of doubly even codes:

Let K, L, M be pairwise disjoint finite sets and $I := K \cup L$, $J := K \cup M$. Furthermore let $C \subset \mathbb{F}_2^I$ be a doubly even linear code and H a linear subspace of C supported by L. We consider H as a code in $\mathbb{F}_2^L$. Obviously every word c of C has the form $c_1 + c_2$ with $c_1 \in \mathbb{F}_2^K$, $c_2 \in H^\perp$. For $\mathfrak{c} \in H^\perp/H$ we define the weight

$$w(\mathfrak{c}) := \min\{|c| \mid c \in \mathfrak{c}\}.$$

Since H is doubly even, we have

$$|c_1| \equiv |c_2| \pmod 4 \qquad \text{for} \quad c_1, c_2 \in \mathfrak{c}.$$

Let D be a doubly even linear code in $\mathbb{F}_2^M$ such that there is an isomorphism ψ of $H^\perp/H$ onto $D^\perp/D$ with

$$w(\psi(\mathfrak{c})) \equiv w(\mathfrak{c}) \pmod 4 \qquad \text{for} \quad \mathfrak{c} \in H^\perp/H.$$

We call such an isomorphism doubly even.

We define the modification C_ψ of C by means of ψ in the following way. C_ψ is the linear subspace of $\mathbb{F}_2^J$ consisting of all words $c_1 + d_2$, $c_1 \in \mathbb{F}_2^K$, $d_2 \in D^\perp$, such that there is a word $c_1 + c_2 \in C$ with $\bar{d}_2 = \psi(\overline{c_2})$.

By definition of ψ it is clear that C_ψ is a doubly even linear code. If C is self-dual, then C_ψ is self-dual and

$$\dim D - |M|/2 = \dim H - |L|/2.$$

(b) The self-dual doubly even codes of length 24 are well known [2]. Up to equivalence there are 9 such codes, which are characterized by their tetrad systems. In the notation of [2] these are the systems: $\varnothing$, $6d_4$, $4d_6$, $3d_8$, $2d_{12}$, d_{24}, $3e_8$, $d_{16} + e_8$, $d_{10} + 2e_7$.

The empty tetrad system corresponds to the Golay code.

(c) It is easy to see that all binary doubly even $(15, 4)$-codes of minimal weight 8 are equivalent. We construct such a code starting from the Reed–Muller code $\mathscr{R}(1, 4)$ which is a $(16, 5)$-code. The positions of this code are the vectors in $\mathbb{F}_2^4$ and the code words are given by the linear polynomials in $\mathbb{F}_2[x_1, x_2, x_3, x_4]$. From $\mathscr{R}(1, 4)$ we go over to a $(15, 4)$-code H by removing the position $(0, 0, 0, 0)$. The polynomials x_1, x_2, x_3, x_4 form a basis of H, and the automorphism group of H is $\mathrm{GL}_4(\mathbb{F}_2)$.

In the factor space $B := H^{\perp}/H$ we have the following structure:

(i) The bilinear form $\langle\ ,\ \rangle\colon B \times B \to \mathbb{F}_2$, induced from the bilinear form in $H^{\perp}$.

(ii) The weight of $\bar{c} \in B$, defined as the minimal weight of the elements in the class $\bar{c}$.

(iii) The action of $\mathrm{GL}_4(\mathbb{F}_2)$, induced from the automorphism group of H.

B contains 8 orthogonal bases formed by elements of weight 5. One of them is given by the polynomials

$$b_1 = 1 + x_1x_2 + x_2x_3 + x_3x_4, \qquad b_2 = 1 + x_1x_2 + x_1x_4 + x_3x_4,$$
$$b_3 = 1 + x_1x_3 + x_1x_2 + x_2x_4, \qquad b_4 = 1 + x_1x_3 + x_3x_4 + x_2x_4,$$
$$b_5 = 1 + x_1x_4 + x_1x_3 + x_2x_3, \qquad b_6 = 1 + x_1x_4 + x_2x_4 + x_2x_3,$$
$$b_7 = 1 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

The others are then given by

$$b_i,\ 1 + b_i + b_1,\ \ldots,\ 1 + b_i + b_{i-1},\ 1 + b_i + b_{i+1},\ \ldots,\ 1 + b_i + b_7$$

for $i = 1, 2, \ldots, 7$.

The weight of the sum of s pairwise different basis elements is equal to s (resp. $s+4$) if $s > 2$ (resp. $s \leqslant 2$).

LEMMA 1. $\mathrm{GL}_4(\mathbb{F}_2)$ *acts effectively on* B.

Proof. Let $\sigma \in \mathrm{GL}_4(\mathbb{F}_2)$ with $\sigma(\bar{b}_i) = \bar{b}_i$ for $i = 1, \ldots, 7$. σ has the form

$$\sigma(x_i) = \sum_{k=1}^{4} \alpha_{ik} x_k, \qquad \alpha_{ik} \in \mathbb{F}_2,$$

with

$$\sigma(x_i)\,\sigma(x_j) = x_i x_j \pmod{H} \qquad \text{for} \quad i \neq j.$$

From this we get the equations

$$\alpha_{ik}\alpha_{jl} + \alpha_{il}\alpha_{jk} = 0 \qquad \text{for} \quad \{i, j\} \neq \{k, l\},\ i \neq j,\ k \neq l, \tag{1}$$

$$\alpha_{ii}\alpha_{jj} + \alpha_{ij}\alpha_{ji} = 1 \qquad \text{for} \quad i \neq j. \tag{2}$$

Assume that for some index t we have $\alpha_{tt} = 0$. Then it follows from (2) that $\alpha_{tj} = \alpha_{jt} = 1$ for $j \neq t$ and from (1) that $\alpha_{tl}\alpha_{jt} = 0$ for $j \neq l$, $j \neq t$, $l \neq t$. This is

a contradiction. So we have $\alpha_{tt} = 1$ for all t, and from (1), (2) we get the equations

$$\alpha_{jl} = \alpha_{il}\alpha_{ji} \quad \text{for} \quad j \neq l,\ i \neq l,\ j \neq i, \tag{3}$$

$$\alpha_{ij}\alpha_{ji} = 0 \quad \text{for} \quad i \neq j. \tag{4}$$

From (3) it follows that if $\alpha_{st} = 1$ for some s, t with $s \neq t$, then $\alpha_{si} = \alpha_{it} = 1$ for all i. This contradicts (4). Q.E.D.

It is easy to see that $\mathrm{GL}_4(\mathbb{F}_2)$ acts transitively on the 8 orthogonal bases formed by elements of weight 5. Therefore, from Lemma 1 it follows that a subgroup P of $\mathrm{GL}_4(\mathbb{F}_2)$ of order $\frac{15\cdot 4\cdot 12\cdot 8}{8} = \frac{7!}{2}$ acts as permutation group on $\{\bar{b}, ..., \bar{b}_7\}$. Hence this must be the alternative group A_7.

Furthermore let $\sigma_i \in \mathrm{Aut}(B)$ be defined for $i = 1, ..., 7$ by $\sigma_i(\bar{b}) = \bar{b}_i$, $\sigma_i(\bar{b}_j) = \bar{1} + \bar{b}_i + \bar{b}_j$, $j \neq i$. Following Conway and Pless [2] we call σ_i an inversion. It is easy to see that σ_i multiplied by an odd permutation of S_7 is in $\mathrm{GL}_4(\mathbb{F}_2)$.

With this preparation now we can prove Theorem 1. Let C be a CP-code containing a (15, 4)-code H. Let 1, ..., 15 be the positions of H and 16, ..., 32 the other positions of C. Furthermore, let $M = \{a_1, ..., a_7\}$ be a set of seven places. Then we define a doubly even isomorphism ψ of $B = H^{\perp}/H$ onto $\mathbb{F}_2^M$ by $\psi(\bar{b}_i) = \{a_i\}$ for $i = 1, ..., 7$. The modified code C_ψ is a doubly even, self-dual code of length 24. On the other hand, starting with a doubly even, self-dual code C with positions $a_1, ..., a_7$, 16, ..., 32 we get by modification with ψ^{-1} a doubly even, self-dual code $C^* = C_{\psi^{-1}}$ with the positions 1, ..., 32. In this manner we can get a CP-code only if C is the Golay code or the code with tetrad system $6d_4$. In fact each tetrad of C must contain one of the places $a_1, ..., a_7$ and no more than two, since the corresponding words in C^* must have weight $\geqslant 8$. If the tetrad system of C has a component d_{2s}, then the support of this component contains not less than $s-1$ of the places $a_1, ..., a_7$. Correspondingly, a component e_7 (resp. e_8) contains not less than 3 (resp. 4) such places. Hence the list of tetrad systems in (b) shows that only the cases $\varnothing$ and $6d_4$ are possible.

In the case $6d_4$ up to equivalence (with respect to C^*) we must have the tetrads

$$\{a_1, 16, 17, 18\}, \quad \{a_2, 19, 20, 21\}, \quad \{a_3, 22, 23, 24\},$$

$$\{a_4, 25, 26, 27\}, \quad \{a_5, 28, 29, 30\}, \quad \{a_6, a_7, 31, 32\}.$$

Using instead of ψ the doubly even isomorphism $\psi\sigma_7$ we go over to the Golay code, since the words in C of length 8 contain the positions in the tetrads always pairwise.

So we can forget about the case $6d_4$ and consider only the Golay code. We remember that for 5 positions given arbitrarily, the Golay code

contains exactly one code word of weight 8 with this position. Therefore, we have to consider three possibilities:

(a) There is a code word of weight 8 in C containing $\{a_1, ..., a_7\}$.

(b) There is a code word of weight 8 in C containing exactly 6 of the 7 positions $a_1, ..., a_7$.

(c) There is no code word of weight 8 in C containing more than 5 of the positions $a_1, ..., a_7$.

Ad (a). Up to equivalence, in a unique way we can choose the following code words of weight 8 of C, always prescribing the first five positions:

$$\begin{array}{ll} \{a_1, ..., a_7, 16\}, & \{a_1, a_2, a_3, a_4, 17, 18, 19, 20\}, \\ \{a_1, a_2, a_3, a_5, 17, 21, 22, 23\}, & \{a_1, a_2, a_3, a_6, 17, 24, 25, 26\}, \\ \{a_1, a_2, a_4, a_5, 17, 24, 27, 28\}, & \{a_1, a_2, a_4, a_6, 17, 21, 29, 30\}, \\ \{a_1, a_2, a_5, a_6, 17, 18, 31, 32\}, & \{a_1, a_3, a_4, a_5, 17, 25, 29, 32\}, \\ \{a_1, a_3, a_4, a_6, 17, 22, 27, 32\}, & \{a_1, a_3, a_5, a_6, 17, 19, 28, 30\}. \end{array} \quad (5)$$

Systematically, it follows the word $\{a_1, a_4, a_5, a_6, 17, 20, 23, 26\}$, but this is linearly dependent on the previously chosen words. We proceed with

$$\{a_2, a_3, a_4, a_5, 17, 26, 30, 32\}.$$

There are two possibilities to complete the positions $a_1, a_2, a_3, 16, 17$ to a word of weight 8 compatible to the already chosen code words:

$$\{a_1, a_2, a_3, 16, 17, 28, 29, 32\} \text{ and } \{a_1, a_2, a_3, 16, 17, 27, 30, 31\}. \quad (6)$$

(These choices are equivalent with respect to C. We can apply, for instance the permutation $(a_4, a_5)(18, 21)(19, 22)(20, 23)(27, 28)(29, 31)(30, 32)$. This shows the uniqueness of the Golay code. But we do not know whether there are equivalent with respect to C^*, and as will be seen at the end of this section, they are in fact not equivalent.)

It is easy to see that the 12 words which we have chosen are linearly independent. It follows that in case (a), we have up to equivalence no more than two CP-codes.

Ad (b). We apply the permutation $(a_7, 17)$ to (a) and get two CP-codes with a code word containing exactly 6 of the 7 positions $a_1, ..., a_7$. But these codes are equivalent. They are transformed into each other by the permutation (16, 17).

Ad (c). We choose the words

$$\begin{aligned}
&\{a_1, a_2, a_3, a_4, a_5, 16, 17, 18\}, \qquad \{a_1, a_2, a_3, a_4, a_6, 19, 20, 21\},\\
&\{a_1, a_2, a_3, a_4, a_7, 22, 23, 24\}, \qquad \{a_1, a_2, a_3, a_5, a_6, 22, 25, 26\},\\
&\{a_1, a_2, a_3, a_5, a_7, 19, 27, 28\}, \qquad \{a_1, a_2, a_3, a_6, a_7, 16, 29, 30\},\\
&\{a_1, a_4, a_5, a_6, a_7, 16, 19, 22\}.
\end{aligned} \tag{7}$$

Now it is impossible to complete the positions a_2, a_3, a_4, a_5, a_6 to a word of weight 8 which is compatible with the previous chosen words. Hence case (c) cannot appear.

Summing up, we see that there are no more than three CP-codes containing a (15, 4)-code. On the other hand, RM, F, and G are such codes. RM and F contain even a (16, 5)-code and belong therefore to case (a).

For the code G, the following scheme shows 15 positions + it is the support of 4 linearly independent code words:

$$\begin{array}{cccc|cccc}
0 & + & + & + & 0 & 0 & 0 & 0\\
+ & 0 & 0 & 0 & 0 & + & + & +\\
+ & 0 & 0 & 0 & 0 & + & + & +\\
+ & 0 & 0 & 0 & 0 & + & + & +
\end{array} \tag{8}$$

This proves Theorem 1.

3. Verification of Table I

We begin the verification of the table with the third row and consider the first two rows at the end of this section.

Row 3. The configuration consists of the code-words

(1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 4, 17, 18, 19, 20; 5, 9, 13, 17, 21; 5, 10, 14, 18, 22; 5, 11, 15, 19, 23),

where we put $d = 4$, $e = 5$. We have four linearly independent code words of weight 8 with support $\{9, 10, \ldots, 23\}$:

$$\begin{aligned}
&(9, 10, 11, 12; 13, 14, 15, 16; 17, 18, 19, 20)\\
&(9, 13, 17, 21; 10, 14, 18, 22; 11, 15, 19, 23).
\end{aligned} \tag{9}$$

Therefore by Theorem 1 our code must be equivalent to RM, F, or G. But RM and F do not have configuration 3, and only G remains.

Row 4. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 4, 17, 18, 19, 20; 21, 5, 9, 13 17; 21, 6, 10, 14, 18; 21, 7, 11, 15, 19) with $d=4$, $e=21$. The sum of the seven code words of the configuration gives $\{1, 2, 3, 8, 12, 16, 21\}$, a contradiction to Theorem 2.

Row 5. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 4, 17, 18, 19, 20; 5, 9, 13, 17, 21; 5, 10, 14, 18, 22; 6, 9, 15, 19, 22) with $d=4$, $e=5$, $f=9$. We have three linearly independent code words of weight 8 with support in the code word $\{1, ..., 16\}$. Hence by Theorem 3 there are also three linearly independent code words of weight 8 with support in $\{17, ..., 32\}$. Up to equivalence they must have the form (17, 20, 21, 23; 18, 19, 22, 24; 25, 26, 27, 28; 29, 30, 31, 32). Then we have the code word

$$\{1, 2, 3, 4, 17, 18, 19, 20\} + \{17, 20, 21, 23, 18, 19, 22, 24\} = \{1, 2, 3, 4, 21, 22, 23, 24\}, \tag{10}$$

in contradiction to Theorem 2.

Row 6. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 4, 17, 18, 19, 20; 5, 9, 13, 17, 21; 5, 10, 14, 18, 22; 6, 9, 14, 19, 23) with $d=4$, $e=5$, $f=9$, $g=14$. There are three linearly independent code words of weight 8 with support in $\{1, 2, 3, 4, 21, ..., 32\}$:

$$(4, 21, 22, 23; 1, 24, 25, 26; 2, 27, 28, 29; 3, 30, 31, 32). \tag{11}$$

Each of the following three code words contain three linearly independent code words of weight 8, which we consider simultaneously:

$$\{5, 6, 7, 8, 21, ..., 32\}, \{9, 10, 11, 12, 21, ..., 32\}, \{13, 14, 15, 16, 21, ..., 32\}. \tag{12}$$

Up to equivalence we have two possibilities to choose these words:

(a) (21, 22, 23, 24; 5, 6, 27, 30; 9, 10, 28, 31; 13, 14, 29, 32),
(5, 21, 22, 24; 7, 25, 28, 29; 8, 26, 31, 32),
(9, 21, 23, 24; 11, 25, 27, 29; 12, 26, 30, 32),
(14, 22, 23, 24; 15, 25, 27, 28; 16, 26, 30, 31).

(b) (21, 22, 23; 5, 6, 24, 27, 30; 9, 10, 24, 28, 31; 13, 14, 25, 27, 31),
(5, 21, 22, 27; 7, 25, 26, 29; 8, 28, 31, 32),
(9, 21, 23, 24; 11, 26, 30, 32; 12, 25, 27, 29),
(14, 22, 23, 31; 15, 24, 26, 30; 16, 28, 29, 32).

Now it is easy to see that in both cases the chosen words generate a subspace of dimension 16 in $\mathbb{F}_2^{32}$. Therefore, there cannot be more than two non-equivalent CP-codes with configuration 6.

Row 7. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 10, 13, 17, 18; 5, 11, 14, 19, 20; 6, 9, 15, 17, 19; 7, 9, 16, 18, 20) with $d=4$, $e=5$, $f=9$. The sum of the last six code words is $\{6, 7, 9, 12\}$.

Row 8. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 11, 15, 17, 19; 6, 12, 16, 18, 20) with $d=4$, $e=5$, $f=6$. We have the following four linearly independent code words with support in $\{4, 5, 6, 9, ..., 20\}$:

(4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 11, 15, 17, 19). (13)

Row 9. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 10, 13, 17, 18; 6, 9, 14, 17, 19; 7, 11, 15, 17, 20; 5, 9, 16, 20, 21) with $d=4$, $e=17$, $f=5$, $g=9$. There are three linearly independent code words of weight 8 with support in $\{17, ..., 32\}$ and therefore two code words of weight 8 with 17 in its support. But in each such word one must have also 18, 19, 20, 21 in the support. It follows that there can be only one such code word.

Row 10. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 9, 15, 19, 21; 6, 11, 16, 17, 20) with $d=4$, $e=5$, $f=6$, $g=9$. This case is analogous to 9.

Row 11. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 14, 17, 18; 5, 10, 13, 19, 20; 6, 9, 15, 21; 6, 11, 13, 17, 22) with $d=4$, $e=5$, $f=6$, $g=9$, $h=13$. There are three linearly independent code words of weight 8 with support in $\{17, ..., 32\}$: (17, 18, 22, 23; 19, 20, 21, 24; 25, 26, 27, 28; 29, 30, 31, 32).

Now we have four linearly independent code words with support in the code word $\{9, ..., 24\}$. Therefore, there are four linear independent code words of weight 8 with support in $\{1, ..., 8, 25, ..., 32\}$. A code word of weight 8 with 4 in its support, lying in $\{1, ..., 8, 25, ..., 32\}$, must also contain 5 and 6. This gives the desired contradiction.

Row 12. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 9, 15, 19, 21; 6, 10, 16, 17, 22) with $d=4$, $e=5$, $f=6$, $g=9$, $h=10$. This case is analogous to 11.

Row 13.

(1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; 5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 9, 15, 19, 21; 6, 10, 13, 22, 23) (14)

with $d=4$, $e=5$, $f=6$, $g=9$, $h=10$, $i=13$. There are three linearly independent code words of weight 8 with support in $\{17, ..., 32\}$:

(19, 20, 21, 24; 17, 18, 25, 26; 22, 23, 27, 28; 29, 30, 31, 32). (15)

(1, 2, 3, 13; 4, 14, 15, 16; 5, 9, 17, 18; 6, 10, 22, 23) implies three linearly independent code words of weight 8 with support in $\{7, 8, 11, 12, 19, 20, 21, 24, ..., 32\}$:

$$(19, 20, 21, 29;\quad 24, 30, 31, 32;\quad 7, 8, 25, 27;\quad 11, 12, 26, 28). \tag{16}$$

The other numbers in our configuration which appear three times give no new code word with the same procedure. We consider (7, 8, 11, 12; 25, 26, 27, 28; 14, 15, 20, 21; 5, 6, 9, 10).

This implies three linearly independent code words of weight 8 with support in $\{1, 2, 3, 4, 13, 16, 17, 18, 19, 22, 23, 24, 29, 30, 31, 32\}$:

$$(1, 13, 16, 24;\quad 2, 17, 22, 31;\quad 3, 18, 23, 32;\quad 4, 19, 29, 30). \tag{17}$$

Furthermore from

(7, 8, 17, 18; 4, 6, 9, 13; 14, 16, 19, 21; 11, 12, 22, 23; 24, 26, 27, 29),

we get now code words

$$(5, 10, 15, 20;\quad 1, 24, 29, 30;\quad 2, 25, 28, 31;\quad 3, 26, 27, 32), \tag{18}$$

$$(5, 15, 28, 31;\quad 1, 11, 23, 30;\quad 2, 10, 20, 25;\quad 3, 12, 22, 32), \tag{19}$$

$$(5, 20, 28, 2;\quad 1, 7, 18, 30;\quad 10, 15, 25, 31;\quad 3, 8, 17, 32). \tag{20}$$

The constructed code words generate a code of dimension 16. Since the construction is unique up to equivalence there is no more than one CP-code with the given configuration.

Row 14. (1, 2, 3; 4, 5, 6, 7, 8; 4, 9, 10, 11, 12; 4, 13, 14, 15, 16; (5, 9, 13, 17, 18; 5, 10, 14, 19, 20; 6, 9, 14, 21, 22; 6, 10, 13, 23, 24) with $d=4$, $e=5$, $f=6$, $g=9$, $h=10$, $i=13$, $j=14$. There are three linearly independent code words of weight 8 with support in $\{17, ..., 32\}$: (17, 18, 19, 20; 21, 22, 23, 24; 25, 26, 27, 28; 29, 30, 31, 32). (1, 2, 3, 9; 4, 10, 11, 12; 5, 13, 17, 18; 6, 14, 21, 22) implies (7, 8, 15, 16; 19, 20, 23, 24; 25, 26, 29, 30; 27, 28, 31, 32).

(The uniqueness up to equivalence comes from the high symmetry of the configuration. We can consider the numbers 4, 5, 6, 9, 10, 13, 14 as the points of the projective plane $\mathbb{P}^2(\mathbb{F}_2)$ and the pairs 7, 8; 11, 12; 15, 16; 17, 18; 19, 20; 21, 22; 23, 24 as the lines of $\mathbb{P}^2(\mathbb{F}_2)$.)

Now we have four linearly independent code words of weight 8 with support $\{17, ..., 32\}$. We can write them in the following convenient way: (17, 18 | 19, 20; 21, 22 | 23, 24; 25, 26 | 27, 28; 29, 30 | 31, 32).

We get the 14 code words with support in $\{17, ..., 32\}$ combining two tretrads or combining from each tetrad one pair such that the front pairs of

the tetrads appear in even numbers. Up to equivalence we have two possibilities for the corresponding code word of weight 8 with support in $\{1, ..., 16\}$:

(a) (3, 4|1, 2; 5, 6|7, 8; 9, 10|11, 12; 13, 14|15, 16)

(b) (3, 4|1, 2; 5, 7|6, 8; 9, 11|10, 12; 13, 15|14, 16).

In case (a) we consider

(1, 2, 17, 18; 3, 5, 9, 13; 4, 6, 10, 14; 11, 12, 21, 22; 15, 16, 23, 24).

It implies that there are three linearly independent code words of weight 8 with support in $\{3, 5, 7, 8, 9, 13, 19, 20, 25, ..., 32\}$:

(3, 5, 9, 13; 7, 8, 19, 20; 25, 27, 29, 31; 26, 28, 30, 32).

Now we have five linearly independent code words of weight 8 with support in $\{3, 4, 5, 6, 9, 10, 13, 14, 25, ..., 32\}$:

(3, 5|9, 13; 4, 6|10, 14; 25, 27|29, 31; 26, 28|30, 32)

and $\{3, 4, 9, 10, 25, 26, 29, 30\}$. Hence it follows from Theorem 1 that our code can only be the CP-code F.

In case (b) we have the code word

$$\{3, 7, 11, 13, 14, 16, 17, 18\}$$
$$= \{4, 5, 9, 14, 15, 16, 17, 18\} + \{3, 4, 5, 7, 9, 11, 13, 15\}$$

and therefore (3, 7, 11, 16; 13, 14, 17, 18; 9, 10, 19, 20; 5, 6, 21, 22). This implies (4, 8, 12, 15; 1, 2, 23, 24; 25, 27, 29, 31; 26, 28, 30, 32). Now we have four linear independent code words of weight 8 with support in $\{4, 7, 8, 11, 12, 15, 16, 25, ..., 32\}$:

$$\{11, 12, 15, 16, 25, 26, 27, 28\}, \quad \{11, 12, 15, 16, 29, 30, 31, 32\},$$

$$\{7, 8, 15, 16, 25, 26, 29, 30\}, \quad \{4, 8, 12, 15, 25, 27, 29, 31\}.$$

Hence it follows from Theorem 1 that our code is the CP-code G or F:

$$1. \quad (1, 2, 3, 4; 5, 6, 7, 8; ...; 29, 30, 31, 32). \tag{21}$$

We can assume that we only have configurations 1 or 2 in the code. A code word of weight 8 is contained in (21) or contains a pair of numbers in four tetrads of (21) or contains one number in each tetrad. Suppose that there are four tetrads with more than 14 code words of weight 8 in the corresponding support. Then we can apply Theorem 1. Therefore we can

assume that in all sets of four tetrads there are no more than 14 code words of weight 8 in the corresponding support. This gives $8 \cdot \binom{8}{4} + \binom{8}{2} = 588$ code words of weight 8. Since there are 620 code words of weight 8 there exists a word of the third type in the code: $\{1, 5, 9, 13, 17, 21, 25, 29\}$. Since we have only configurations 1 and 2 we can assume that there are five code words of weight 8 containing 1, 5, 9, 13. Therefore $\{1, ..., 16\}$ or $\{17, ..., 32\}$ contains five linearly independent code words of weight 8 and we can apply Theorem 1

2. (1, 2, 3, 4; 5, 6, 7, 8; ...; 21, 22, 23, 24; 4, 5, 9, 13, 17, 21; 4, 5, 10, 14, 18, 22) with $d=4$, $e=5$. Now we can assume that we only have the configuration 2 in the code. Up to equivalence we therefore have also the following words in the code:

(1, 2, 3, 4; 1, 6, 9, 13, 19, 23; 1, 6, 10, 14, 20, 24; 2, 7, 11, 15, 17, 21; 2, 7, 12, 16, 18, 22; 3, 8, 11, 15, 19, 23; 3, 8, 12, 16, 20, 24).

We have already five code words of weight 8 containing 1, 6, 9:

(1, 6, 9; 13, 17, 18, 20, 23; 13, 19, 21, 22, 24; 13, 3, 8, 11, 15; 14, 15, 16, 19, 23; 14, 11, 12, 20, 24).

Hence there must be two code words c_1, c_2 of the form

$$c_1 = \{1, 6, 9, 13, 14, *, *, *\}, \quad c_2 = \{1, 6, 9, 13, 12, 16, *, *\}.$$

Both have support in $\{1, ..., 16\}$. Therefore. we have five linearly independent code words of weight 8 with support in $\{1, ..., 16\}$. This leads to the desired contradiction.

ACKNOWLEDGMENT

The author would like to thank B. B. Venkov from whom he learned much about self-dual codes.

REFERENCES

1. P. J. CAMERON AND J. H. VAN LINT, 'Graph Theory, Coding Theory and Block Designs," Cambridge Univ. Press, London, 1975.
2. J. H. CONWAY AND V. PLESS, On the enumeration of self-dual codes, *J. Combin. Theory Ser. A* **28** (1980), 26–53.
3. J. H. VAN LINT, "Introduction to Coding Theory," Springer-Verlag, New York/Heidelberg/ Berlin, 1982.
4. N. J. A. SLOANE, Self-dual codes and lattices, *in* "Relations between Combinatorics and Other Parts of Mathematics, Proceedings, Symp. in Pure Math. 34, 1979," pp. 273–308.