Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Discrete Mathematics 282 (2004) 171–182
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Binary codes from graphs on triples

J.D. Key[a,*,1], J. Moori[b,2], B.G. Rodrigues[b,3]

[a]Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA
[b]School of Mathematics, Statistics and Information Technology, University of Natal-Pietermaritzburg, Pietermaritzburg 3209, South Africa

Received 14 November 2002; accepted 4 December 2003

Abstract

For a set Ω of size $n \geqslant 7$ and $\Omega^{\{3\}}$ the set of subsets of Ω of size 3, we examine the binary codes obtained from the adjacency matrix of each of the three graphs with vertex set $\Omega^{\{3\}}$, with adjacency defined by two vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively.

MSC: 05; 51; 94

Keywords: Codes; Graphs; Designs

1. Introduction

The binary codes formed from the span of the adjacency matrix of graphs, and in particular strongly regular graphs, have been examined by various authors: see [4–6,11,1,2]. Here, we examine a different class of graphs and prove the following theorem.

Theorem 1. *Let Ω be a set of size n, where $n \geqslant 7$. Let $\mathscr{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of the three graphs $A_i(n)$, for $i = 0,1,2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in zero, one or two elements, respectively. Let $C_i(n)$ denote the code formed from the row span over F_2 of an adjacency matrix for $A_i(n)$. Then*

(1) $n \equiv 0 \pmod 4$:
  (a) $C_2(n) = F_2^{\mathscr{P}}$;
  (b) $C_0(n) = C_1(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ *and* $C_0(n)^\perp$ *is* $[\binom{n}{3}, n, \binom{n-1}{2}]_2$;
(2) $n \equiv 2 \pmod 4$:
  $C_i(n) = F_2^{\mathscr{P}}$ *for* $i = 0,1,2$;
(3) $n \equiv 1 \pmod 4$:
  (a) $C_0(n) = C_1(n) \cap C_2(n)$;
  (b) $C_0(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ *and* $C_0(n)^\perp$ *is* $[\binom{n}{3}, \binom{n}{2}, n-2]_2$;
    $C_1(9)$ *is* $[84, 76, 3]_2$ *and* $C_1(9)^\perp$ *is* $[84, 8, 38]_2$;
    $C_1(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - n + 1, 4]_2$ *and* $C_1(n)^\perp$ *is* $[\binom{n}{3}, n-1, (n-2)(n-3)]_2$ *for* $n > 9$;
    $C_2(n)$ *is* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *and* $C_2(n)^\perp$ *is* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$;

---

* Corresponding author.
[1] This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565, and NSF Grant #9730992.
[2] Support of NRF and the University of Natal (URF) acknowledged.
[3] Post-graduate scholarship of DAAD (Germany) and the Ministry of Petroleum (Angola) acknowledged.
E-mail address: keyj@clemson.edu (J.D. Key).

doi:10.1016/j.disc.2003.12.004

(4) $n \equiv 3 \pmod 4$:
 (a) $C_1(n) = \langle v^P + \jmath \mid P \in \mathscr{P} \rangle$ *is* $[\binom{n}{3}, \binom{n}{3} - 1, 2]_2$;
 (b) $C_0(n) = C_2(n)$ *is* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *and* $C_2(n)^\perp$ *is* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$.

For all $n \geqslant 7, i = 0,1,2, C_i(n) \cap C_i(n)^\perp = \{0\}$, *and the automorphism groups of these codes are* S_n *or* $S_{\binom{n}{3}}$.

The theorem will follow from a series of lemmas and propositions proved in Section 3. The ideas and methods in this paper are similar to those used in [8] in which binary codes of the triangular graphs were considered, and for which PD-sets for permutation decoding (see [10, Chapter 15], [7, Section 8]) were found. In a following paper [9] we use the codes considered in this present paper for permutation decoding and give explicit PD-sets for some of the infinite families.

2. Background and terminology

Our notation for designs and codes will be standard and as in [1]. An incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, with point set $\mathscr{P}$, block set $\mathscr{B}$ and incidence $\mathscr{I}$ is a t-(v,k,λ) design, if $|\mathscr{P}| = v$, every block $B \in \mathscr{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The number of blocks through a set of s points is denoted by λ_s and is independent of the set if $s \leqslant t$. We will say that the design is *symmetric* if it has the same number of points and blocks.

The *code* C_F *of the design* $\mathscr{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathscr{D}$ is denoted by $\mathscr{P}$ and the block set by $\mathscr{B}$, and if $\mathscr{Q}$ is any subset of $\mathscr{P}$, then we will denote the incidence vector of $\mathscr{Q}$ by $v^{\mathscr{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathscr{B} \rangle$, and is a subspace of $V = F^{\mathscr{P}}$, the full vector space of functions from $\mathscr{P}$ to F. For any vector $w \in V$, the coordinate of w at the point $P \in \mathscr{P}$ is denoted by $w(P)$.

All our codes here will be *linear codes*, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n,k,d]_q$ to show this information. A *generator matrix* for the code is a $k \times n$ matrix made up of a basis for C. The *dual* or *orthogonal* code $C^\perp$ is the orthogonal under the standard inner product (,), i.e. $C^\perp = \{v \in F^n | (v,c) = 0 \text{ for all } c \in C\}$. A *check* (or *parity-check*) matrix for C is a generator matrix H for $C^\perp$. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and is *self-dual* if $C = C^\perp$. If c is a codeword then the *support* of c is the set of non-zero coordinate positions of c. A *constant vector* is one for which all the coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code. Two linear codes of the same length and over the same field are *equivalent* if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are *isomorphic* if they can be obtained from one another by permuting the coordinate positions. An *automorphism* of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$. Any automorphism clearly preserves each weight class of C.

Terminology for *graphs* is standard: the graphs, $\Gamma = (V,E)$ with vertex set V and edge set E, are undirected and the *valency* of a vertex is the number of edges containing the vertex. A graph is *regular* if all the vertices have the same valency.

3. The binary codes

Let n be any integer and Ω a set of size n; to avoid degenerate cases we take $n \geqslant 7$. Taking the set $\Omega^{\{3\}}$ to be the set of all 3-element subsets of Ω, we define three non-trivial undirected graphs with vertex set $\mathscr{P} = \Omega^{\{3\}}$, and denote these graphs by $A_i(n)$ where $i = 0,1,2$. The edges of the graph $A_i(n)$ are defined by the rule that *two vertices are adjacent in* $A_i(n)$ if as 3-element subsets they have exactly i elements of Ω in common. For each $i = 0,1,2$ we define from $A_i(n)$ a 1-design $\mathscr{D}_i(n)$, on the point set $\mathscr{P}$ by defining for each point $P = \{a,b,c\} \in \mathscr{P}$ a block $\overline{\{a,b,c\}}_i$ by

$$\overline{\{a,b,c\}}_i = \{\{x,y,z\} \mid |\{x,y,z\} \cap \{a,b,c\}| = i\}.$$

Denote by $\mathscr{B}_i(n)$ the block set of $\mathscr{D}_i(n)$, so that each of these is a symmetric 1-design on $\binom{n}{3}$ points with block size, respectively;

- $\binom{n-3}{3}$ for $\mathscr{D}_0(n)$;
- $3\binom{n-3}{2}$ for $\mathscr{D}_1(n)$;
- $3(n-3)$ for $\mathscr{D}_2(n)$.

The incidence vector of the block $\overline{\{a,b,c\}}_i$ for $i=0,1,2$, respectively, is then

$$v^{\overline{\{a,b,c\}}_0} = \sum_{x,y,z\in\Omega\setminus\{a,b,c\}} v^{\{x,y,z\}}, \tag{1}$$

$$v^{\overline{\{a,b,c\}}_1} = \sum_{x,y\in\Omega\setminus\{a,b,c\}} v^{\{a,x,y\}} + \sum_{x,y\in\Omega\setminus\{a,b,c\}} v^{\{b,x,y\}} + \sum_{x,y\in\Omega\setminus\{a,b,c\}} v^{\{c,x,y\}}, \tag{2}$$

$$v^{\overline{\{a,b,c\}}_2} = \sum_{x\in\Omega\setminus\{a,b,c\}} v^{\{a,b,x\}} + \sum_{x\in\Omega\setminus\{a,b,c\}} v^{\{a,c,x\}} + \sum_{x\in\Omega\setminus\{a,b,c\}} v^{\{b,c,x\}}, \tag{3}$$

where, as usual with the notation from [1], the incidence vector of the subset $X\subseteq\mathscr{P}$ is denoted by v^X. Since our points here are actually triples of elements from Ω, we emphasize that we are using the notation $v^{\{a,b,c\}}$ instead of the more cumbersome $v^{\{\{a,b,c\}\}}$, as mentioned in [1].

We will be examining the binary codes of these designs; in fact, computation with Magma [3] shows that the codes over some other primes, in particular, $p=3$, might be interesting, but here we consider only the binary codes. Thus, denoting the block set of $\mathscr{D}_i(n)$ by $\mathscr{B}_i(n)$ we will write

$$C_i(n) = C_2(\mathscr{D}_i(n)) = \langle v^b \mid b\in\mathscr{B}_i(n)\rangle,$$

where the span is taken over F_2. Notice that, since the blocks of the three designs do not overlap, we have, for any point $P=\{a,b,c\}$,

$$\jmath = v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1} + v^{\overline{\{a,b,c\}}_2}. \tag{4}$$

Now consider, for any given point $P=\{a,b,c\}\in\mathscr{P}$, the vector

$$w_P = \sum_{P\in b_i} v^{b_i}, \tag{5}$$

i.e. the sum of all the incidence vectors of blocks of $\mathscr{D}_i(n)$ that contain P, for each $i=0,1,2$. For any point Q of $\mathscr{P}$, $w_P(Q)$ (the coordinate of w_P at Q) is determined by four distinct cases, depending on the size of the intersection of the triples that define P and Q. We look at the various cases, writing b_i for a block of $\mathscr{D}_i(n)$:

- $i=0$;
  (1) $P=Q$, $w_P(P)=|b_0|=\binom{n-3}{3}$;
  (2) $|P\cap Q|=2$, $w_P(Q)=\binom{n-4}{3}$, and there are $3(n-3)$ such points;
  (3) $|P\cap Q|=1$, $w_P(Q)=\binom{n-5}{3}$, and there are $3\binom{n-3}{2}$ such points;
  (4) $|P\cap Q|=0$, $w_P(Q)=\binom{n-6}{3}$, and there are $\binom{n-3}{3}$ such points.
- $i=1$;
  (1) $P=Q$, $w_P(P)=|b_1|=3\binom{n-3}{2}$;
  (2) $|P\cap Q|=2$, $w_P(Q)=2\binom{n-4}{2}+(n-4)$, and there are $3(n-3)$ such points;
  (3) $|P\cap Q|=1$, $w_P(Q)=\binom{n-5}{2}+4(n-5)$, and there are $3\binom{n-3}{2}$ such points;
  (4) $|P\cap Q|=0$, $w_P(Q)=9(n-6)$, and there are $\binom{n-3}{3}$ such points.
- $i=2$;
  (1) $P=Q$, $w_P(P)=|b_2|=3(n-3)$;
  (2) $|P\cap Q|=2$, $w_P(Q)=(n-4)$, and there are $3(n-3)$ such points;
  (3) $|P\cap Q|=1$, $w_P(Q)=0$, and there are $3\binom{n-3}{2}$ such points;
  (4) $|P\cap Q|=0$, $w_P(Q)=0$, and there are $\binom{n-3}{3}$ such points.

Congruences modulo 4 give different properties of the binary codes of the designs, as the lemmas to follow will show. As a direct consequence of the observations above for w_P we have:

Lemma 1. *With notation as defined above*, $P=\{a,b,c\}\in\mathscr{P}$,

(1) $n\equiv 0 \pmod 4$:
  (a) *for* $i=0$, $w_P = v^{\overline{\{a,b,c\}}_1}$, *so* $C_1(n)\subseteq C_0(n)$;
  (b) *for* $i=1$, $w_P = v^{\overline{\{a,b,c\}}_1}$;
  (c) *for* $i=2$, $w_P = v^P$, *so* $C_2(n)=F_2^{\mathscr{P}}$.

(2) $n \equiv 2 \pmod 4$: *for* $i = 0,1,2$, $w_P = v^P$, *so* $C_i(n) = F_2^{\mathscr{P}}$.
(3) $n \equiv 1 \pmod 4$:
  (a) *for* $i = 0$, $w_P = v^{\overline{\{a,b,c\}}_0}$;
  (b) *for* $i = 1$, $w_P = v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_2}$, *and* $\jmath \in C_1(n)$;
  (c) *for* $i = 2$, $w_P = v^{\overline{\{a,b,c\}}_2}$.
(4) $n \equiv 3 \pmod 4$:
  (a) *for* $i = 0$, $w_P = v^{\overline{\{a,b,c\}}_2}$, *so* $C_2(n) \subseteq C_0(n)$;
  (b) *for* $i = 1$, $w_P = v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1} + v^{\overline{\{a,b,c\}}_2}$, $w_P = \jmath + v^{\{a,b,c\}}$;
  (c) *for* $i = 2$, $w_P = v^{\overline{\{a,b,c\}}_2}$.

Proof. Follows directly from the observations and Eq. (4). □

Proposition 1. *For* $n \geqslant 7$ *and odd,* $C_2(n)$ *is a* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *code and* $C_2(n)^\perp$ *is a* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$ *code. There are* $\binom{n}{4}$ *words of weight* 4 *in* $C_2(n)$ *and they span the code; there are* $\binom{n}{2}$ *words of weight* $n-2$ *in* $C_2(n)^\perp$ *and they span the code. Furthermore,* $C_2(n) \cap C_2(n)^\perp = \{0\}$.

For n odd $\mathrm{Aut}(C_2(n)) = S_n$. *For n even,* $\mathrm{Aut}(C_2(n)) = S_{\binom{n}{3}}$.

Proof. Since we deal exclusively with $i = 2$ in this proof, we will denote a block of $\mathscr{D}_2(n)$ by $\overline{\{a,b,c\}}$, and write $C = C_2(n)$.

For $\Delta = \{a,b,c,d\}$ any subset of Ω of four elements, let

$$w(a,b,c,d) = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{a,c,d\}} + v^{\{b,c,d\}}. \tag{6}$$

It is quite direct to show that

$$w(a,b,c,d) = v^{\overline{\{a,b,c\}}} + v^{\overline{\{a,b,d\}}} + v^{\overline{\{a,c,d\}}} + v^{\overline{\{b,c,d\}}}$$

and hence $w(a,b,c,d) \in C$. Clearly there are $\binom{n}{4}$ of such words, and the minimum weight of C is at most 4. Furthermore,

$$\sum_{x \in \Omega \setminus \{a,b,c\}} w(a,b,c,x) = \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{a,b,c\}} + \sum_{x \neq c} v^{\{a,b,x\}} + \sum_{x \neq b} v^{\{a,c,x\}} + \sum_{x \neq a} v^{\{b,c,x\}}$$
$$= (n-3) v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}} = 0 + v^{\overline{\{a,b,c\}}}$$

and thus $C = \langle w(a,b,c,d) \mid a,b,c,d \in \Omega \rangle$.

Now we consider the dual code $C^\perp$. For any pair of elements $a,b \in \Omega$, define

$$w(a,b) = \sum_{x \in \Omega \setminus \{a,b\}} v^{\{a,b,x\}}. \tag{7}$$

The weight of $w(a,b)$ is clearly $n-2$; we show it is in $C^\perp$. For any $\overline{\{x,y,z\}} \in \mathscr{B}_2$, writing $w = w(a,b)$,

$$(w, v^{\overline{\{x,y,z\}}}) = \left(w, \sum_{c \neq x,y,z} v^{\{x,y,c\}} \right) + \left(w, \sum_{c \neq x,y,z} v^{\{x,z,c\}} \right) + \left(w, \sum_{c \neq x,y,z} v^{\{y,z,c\}} \right).$$

If $a,b \notin \{x,y,z\}$ then all three terms are 0; if $x = a$ and $b \notin \{x,y,z\}$, the first and second terms are 1, the last term is 0, and hence the sum is 0; if $a,b \in \{x,y,z\}$, then the first term is $n-3 = 0$, and the other two terms are 0, so the sum is 0 again. Thus $w(a,b) \in C^\perp$, and clearly there are $\binom{n}{2}$ vectors of this type.

Now we show that this is the minimum weight of $C^\perp$ and that these are the minimum-weight vectors. Suppose $w \in C^\perp$, and suppose that $v^{\{a,b,c\}}$ is in the support of w. Since $(w, w(a,b,c,d))=0$ for all choices of $d \in \Omega \setminus \{a,b,c\}$, and $w(a,b,c,d)$ and $w(a,b,c,e)$ have only $v^{\{a,b,c\}}$ in common in their supports, for each $d \in \Omega \setminus \{a,b,c\}$ we get another term in w, and thus its weight is at least $1 + (n-3) = n-2$.

To show that any vector in $C^\perp$ of weight $n-2$ has this form, suppose $w \in C^\perp$ has weight $n-2$. Then $(w, w(a,b,c,d))=0$ implies that $w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + \cdots$. Since $(w, w(a,b,c,x)) = 0$ for all choices of $x \in \Omega \setminus \{a,b,c,d\}$, w has another element from $w(a,b,c,x)$ for each such x, so

$$w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + \begin{cases} v^{\{a,b,e\}} + v^{\{a,b,f\}} + \cdots + v^{\{a,b,n\}} \\ v^{\{b,c,e\}} + v^{\{b,c,f\}} + \cdots + v^{\{b,c,n\}} \\ v^{\{a,c,e\}} + v^{\{a,c,f\}} + \cdots + v^{\{a,c,n\}} \end{cases}$$

for one of these cases. The top case is $w(a,b)$; if one of the other cases holds then $v^{\{a,b,x\}}$ is not in the support for some x, which will give a contradiction unless the weight is greater than $n-2$.

To show that 4 is the minimum weight of C, notice that the block size for $\mathscr{D}_2(n)$ is $3(n-3)$, which is even; thus $\jmath \in C^{\perp}$ and hence all words of C have even weight. We need then to show that C does not have words of weight 2. Suppose $w = v^{\{a,b,c\}} + v^{\{d,e,f\}}$; then since $(w, w(a,b)) = 0$, we must have $\{a,b\} \subset \{d,e,f\}$, and $w = v^{\{a,b,c\}} + v^{\{a,b,d\}}$, where $d \neq c$. But then $(w, w(a,c)) \neq 0$, so we have a contradiction, and C cannot have vectors of weight 2. Now suppose C has a vector w of weight 4 that is not of the form $w(a,b,c,d)$. If $w = v^{\{a,b,c\}} + \cdots$ then $(w, w(a,b)) = 0$ implies that $w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + \cdots$. But we also have $(w, w(b,c)) = 0$, so $w = v^{\{a,b,c\}} + v^{\{a,b,d\}} + v^{\{b,c,e\}} + \cdots$. Now similarly arguing that $(w, w(b,d)) = (w, w(a,c)) = 0$, and assuming the weight of w is 4, we find that $d = e$ and $w = w(a,b,c,d)$.

Now we show that the dimension of C is $\binom{n-1}{3}$. For this we construct a basis of words of weight 4. We introduce an ordering of the points and the spanning weight-4 vectors so that the generating matrix is in upper triangular form. For the point order: $\{1,2,3\}, \{1,2,4\}, \ldots, \{1,2,n-1\}, \{1,3,4\}, \ldots, \{1,3,n-1\}, \ldots, \{1,n-2,n-1\}, \{2,3,4\}, \ldots, \{n-3,n-2,n-1\}$ (which will all be pivot positions), and followed by the remaining $\binom{n-1}{2}$ points $\{1,2,n\}, \{1,3,n\}, \ldots, \{n-2,n-1,n\}$.

The weight-4 vectors for the basis will be ordered as follows: $w(1,2,3,4), w(1,2,4,5), w(1,2,5,6), \ldots, w(1,2,n-1,n), w(1,3,4,5), \ldots, w(1,3,n-1,n), \ldots, w(1,n-2,n-1,n), w(2,3,4,5), w(2,3,5,6), \ldots, w(2,3,n-1,n), \ldots, w(n-3,n-2,n-1,n)$.

Then it is simple to verify that with this ordering of points and spanning vectors we get an upper triangular matrix of rank $\binom{n-1}{3}$. Thus C has dimension at least $\binom{n-1}{3}$.

To prove that this is in fact the dimension, we look at $C^{\perp}$. We can keep the same ordering of the points but we will in fact get the pivot positions in the last $\binom{n-1}{2}$ positions. For the rows of the generating matrix H we take the minimum vectors $w(1,2), w(1,3), \ldots, w(1,n-1), w(2,3), \ldots, w(2,n-1), w(n-2,n-1)$; then H has the form $[A|I_k]$ where $k = \binom{n-1}{2}$. Thus $C^{\perp}$ has dimension at least $\binom{n-1}{2} = \binom{n}{3} - \binom{n-1}{3}$, and the proposition is proved.

To show that $C \cap C^{\perp} = \{0\}$, we show that $C + C^{\perp} = F_2^{\mathscr{P}}$ by showing that every vector of weight 1 can be expressed as a sum of vectors from C and $C^{\perp}$. In fact, if $a,b,c \in \Omega$ are distinct, then

$$\begin{aligned} w(a,b) + w(a,c) + w(b,c) + \overline{v^{\{a,b,c\}}} &= \sum_{x \in \Omega \setminus \{a,b\}} v^{\{a,b,x\}} + \sum_{x \in \Omega \setminus \{a,c\}} v^{\{a,c,x\}} + \sum_{x \in \Omega \setminus \{b,c\}} v^{\{b,c,x\}} + \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{a,b,x\}} \\ &\quad + \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{a,c,x\}} + \sum_{x \in \Omega \setminus \{a,b,c\}} v^{\{b,c,x\}} = v^{\{a,b,x\}} + v^{\{a,b,x\}} + v^{\{a,b,x\}} = v^{\{a,b,x\}} \end{aligned}$$

which is what is required.

Finally, we obtain the automorphism group of $C_2(n)$. It is not difficult to see that $\mathrm{Aut}(A_2(n)) = S_n$ and $S_n \subseteq \mathrm{Aut}(C_2(n))$. Let $g \in \mathrm{Aut}(C_2(n))$. Then g maps triples to triples. Also, since the words having the form $w(a,b) = \sum_{x \in \Omega \setminus \{a,b\}} v^{abx}$ are the words of minimum weight $n-2$ in $C_2(n)^{\perp}$, g maps pairs to pairs. We use these facts to show that $\mathrm{Aut}(C_2(n)) = S_n$.

Let $x \in \Omega$. For arbitrary $a,b \in \Omega$ such that $x \in \Omega \setminus \{a,b\}$, suppose that $\{a,b\}^g = \{c,d\}$. Then $\{a,b,x\}^g = \{c,d,x^*\}$ where $x^* \notin \{c,d\}$. Without loss of generality we may assume that $\{a,x\}^g = \{c,x^*\}$. Then we must have $\{b,x\}^g = \{d,x^*\}$.

Now consider $e,f \in \Omega \setminus \{a,b,c,d,x\}$. Then $\{a,e,x\}^g = \{c,x^*,e^*\}$ where $e^* \notin \{c,x^*\}$. This provides two possible images for $\{e,x\}$, namely

$$\{e,x\}^g = \{c,e^*\} \quad \text{or} \quad \{e,x\}^g = \{x^*,e^*\}.$$

If $\{e,x\}^g = \{c,e^*\}$, then we must have $\{a,e\}^g = \{x^*,e^*\}$ which implies $\{b,e,x\}^g = \{c,x^*,e^*,d\}$, a contradiction. Hence we must have $\{e,x\}^g = \{x^*,e^*\}$ which implies $\{a,e\}^g = \{c,e^*\}$. Thus $\{b,e,x\}^g = \{d,x^*,e^*\}$ and we deduce that $\{b,e\}^g = \{d,e^*\}$. Hence $\{a,b,e\}^g = \{c,d,e^*\}$.

Now assume that $\{a,f,x\}^g = \{c,x^*,f^*\}$ where $f^* \notin \{c,x^*\}$. Then similarly to the above argument we get $\{a,f\}^g = \{c,f^*\}$ and $\{f,x\}^g = \{x^*,f^*\}$. Hence $\{b,f,x\}^g = \{d,x^*,f^*\}$ and $\{e,f,x\}^g = \{e^*,x^*,f^*\}$. Finally, we deduce that $\{e,f\}^g = \{e^*,f^*\}$.

From the above we deduce that g is defined in S_n and $\mathrm{Aut}(C_2(n)) = S_n$. For n even, $C_2(n) = F_2^{\binom{n}{3}}$ which gives the result. $\square$

Lemma 2. *For all* $n \geqslant 7$ $C_0(n)$ *has words of weight* 8. *If* n *is odd,* $w(a,b)=\sum_{x\in\Omega\setminus\{a,b\}} v^{\{a,b,x\}} \in C_0(n)^{\perp}$, *and* $C_0(n) \subseteq C_2(n)$. *If* $n \equiv 3 \pmod 4$, $C_0(n)=C_2(n)$.

Proof. We first show how words of weight 8 can be constructed. In this lemma we use the notation $\overline{\{a,b,c\}}$ to denote a block of $\mathscr{D}_0(n)$.

Let $\Delta=\{a,b,c,d,e,f\}$ be a subset of Ω of six elements. For each partition of Δ into three disjoint 2-element subsets we will get a weight-8 vector. The set Δ will be the point set of a 1-(6,3,4) design with $\lambda_2=2$ or 0. We do this as follows: suppose we take the partition $\pi=\{\{a,b\},\{c,d\},\{e,f\}\}$ of Δ; then the rule for our design will be that points (letters) from the same 2-element member of π will not be together in a block. The eight blocks will thus be

$$b_1=\{a,c,e\},\quad b_2=\{a,c,f\},\quad b_3=\{a,d,e\},\quad b_4=\{a,d,f\}$$

and their complements

$$b_5=\{b,d,f\},\quad b_6=\{b,d,e\},\quad b_7=\{b,c,f\},\quad b_8=\{b,c,e\}.$$

It is then a direct matter to prove that

$$w(\pi)=\sum_{i=1}^{8} v^{b_i}=\sum_{i=1}^{8} v^{\overline{b_i}}, \tag{8}$$

thus giving a vector of weight 8 in $C_0(n)$.

Now take n to be odd, and consider

$$(w(a,b),v^{\overline{\{x,y,z\}}})=\left(\sum_{x\in\Omega\setminus\{a,b\}} v^{\{a,b,x\}},\ \sum_{c,d,e\in\Omega\setminus\{x,y,z\}} v^{\{c,d,e\}}\right)=m.$$

Then

- $m=0$ if $\{a,b\}\subseteq\{x,y,z\}$;
- $m=0$ if $a\in\{x,y,z\}$ and $b\notin\{x,y,z\}$;
- if $\{a,b\}\cap\{x,y,z\}=\emptyset$, then $v^{\{a,b,c\}}$ is in the support of $v^{\overline{\{x,y,z\}}}$ except for $c=x,y,z$. Thus they meet in $n-2-3=n-5$ positions, so that $m=0$ for n odd.

Since from Proposition 1 we have that $C_2(n)^{\perp}=\langle w(a,b)\,|\,a,b\in\Omega\rangle$, we have now shown that $C_2(n)^{\perp}\subseteq C_0(n)^{\perp}$ for n odd, and thus $C_0(n)\subseteq C_2(n)$ for n odd. That equality holds here if $n\equiv 3 \pmod 4$ follows from Lemma 1(4a). □

Lemma 3. *For* $n\geqslant 7$, $C_1(n)$ *has words of weight* 4. *If* $n\equiv 0 \pmod 4$ *then* $C_0(n)$ *has words of weight* 4.

Proof. We define two types of words of $F^{\mathscr{P}}$ of weight 4 and show that they are in $C_1(n)$ for any $n\geqslant 7$.

Let $\Delta=\{a,b,c,d,e,f\}\subseteq\Omega$ of size 6, and let $\Delta^*=[a,b,c,d,e,f]$ be a sequence of the elements of Δ. Let

$$w(\Delta^*)=v^{\{a,b,c\}}+v^{\{a,b,d\}}+v^{\{c,e,f\}}+v^{\{d,e,f\}}. \tag{9}$$

Then it is quite direct to show that

$$w(\Delta^*)=v^{\overline{\{a,b,c\}}}+v^{\overline{\{a,b,d\}}}+v^{\overline{\{c,e,f\}}}+v^{\overline{\{d,e,f\}}},$$

where our notation is for blocks of $\mathscr{D}_1(n)$ in this lemma.

Similarly, let $\Delta=\{a,b,c,d,e\}\subseteq\Omega$ of size 5, and let $\Delta^*=[a,b,c,d,e]$ be a sequence of the elements of Δ. Let

$$u(\Delta^*)=v^{\{a,b,c\}}+v^{\{a,b,d\}}+v^{\{a,c,e\}}+v^{\{a,d,e\}}. \tag{10}$$

Then again it is quite direct to show that

$$u(\Delta^*)=v^{\overline{\{a,b,c\}}}+v^{\overline{\{a,b,d\}}}+v^{\overline{\{a,c,e\}}}+v^{\overline{\{a,d,e\}}},$$

thus illustrating two different types of words of weight 4 in $C_1(n)$ for any n.

Since $C_1(n)\subseteq C_0(n)$ when $n\equiv 0 \pmod 4$ (by Lemma 1(1a)), $C_0(n)$ also has words of weight 4 in this case. □

Note: If we take the sequence $\Delta'=[a,f,c,d,e,b]$ in the first construction of Lemma 3, then

$$w(\Delta^*)+w(\Delta')=w(\pi),$$

where $\pi = \{\{a,e\},\{b,f\},\{c,d\}\}$ is the partition of the set Δ as used in the construction of the weight-8 words in $C_0(n)$ in Lemma 2, and $w(\pi)$ is as defined in Eq. (8).

Lemma 4. *For* $n \equiv 0 \pmod 4$, $C_1(n)^{\perp}$ *has* n *words of weight* $\binom{n-1}{2}$ *given, for each* $a \in \Omega$, *by*

$$w(a) = \sum_{x,y \in \Omega \setminus \{a\}} v^{\{a,x,y\}}. \tag{11}$$

The same is true for $C_0(n)^{\perp}$ *for* $n \equiv 0 \pmod 4$ *and for* $n \equiv 1 \pmod 4$.

For any n, *the* n *vectors* $w(a)$ *are linearly independent and* $\jmath = \sum_{a\in\Omega} w(a)$; *if* $n \equiv 1 \pmod 4$ *then*

$$S = \langle \jmath + w(a) \mid a \in \Omega \rangle \subseteq C_1(n)^{\perp}$$

and has dimension $n-1$.

Proof. Let $w(a)$ be as defined, and consider first $C_1(n)^{\perp}$. Taking an arbitrary block of $\mathscr{D}_1(n)$, consider $(w(a), v^{\overline{\{b,c,d\}}_1}) = m$. Direct computation shows that

- if $a \notin \{b,c,d\}$ then $m = 3(n-4)$;
- if $a \in \{b,c,d\}$ then $m = \binom{n-3}{2}$.

Thus if $n \equiv 0 \pmod 4$, $m = 0$ and $w(a) \in C_1(n)^{\perp}$. If $n \equiv 1 \pmod 4$ then $m = 1$ for all blocks, and since the block size is odd in this case, it follows that $(\jmath, v^{\overline{\{b,c,d\}}_1}) = 1$ and hence that $\jmath + w(a) \in C_1(n)^{\perp}$.

Now consider $C_0(n)^{\perp}$ and let $m = (w(a), v^{\overline{\{b,c,d\}}_0})$. It follows that

- if $a \notin \{b,c,d\}$ then $m = \binom{n-4}{2}$;
- if $a \in \{b,c,d\}$ then $m = 0$.

Thus if $n \equiv 0 \pmod 4$ or if $n \equiv 1 \pmod 4$, we will have $m = 0$ and $w(a) \in C_0(n)^{\perp}$.

Clearly there are n words of this type. We now show that they are linearly independent: suppose

$$\sum_{i=1}^{n} a_i w(i) = 0 = \sum_{i=1}^{n} a_i \sum_{j,k \in \Omega \setminus \{i\}} v^{\{i,j,k\}}.$$

The coefficient of $v^{\{i,j,k\}}$ is $a_i + a_j + a_k = 0$ for every choice of the triple $\{i,j,k\}$. It follows easily that $a_i = 0$ for all i.

That $\jmath = \sum_{a\in\Omega} w(a)$ follows from the observation that each vector $v^{\{a,b,c\}}$ will occur exactly three times in the sum. For n odd then it also follows that $\sum_{a\in\Omega}(\jmath + w(a)) = 0$, completing the proof. □

Lemma 5. *For* $n \equiv 0 \pmod 4$, $C_1(n) = C_0(n)$ *and has minimum weight* 4. *For* $n \equiv 1 \pmod 4$, $C_0(n) \subset C_1(n)$.

Proof. First show that the minimum weight of $C_1(n)$ is 4. Notice that the block size is $3\binom{n-3}{2}$, which is even for $n \equiv 0 \pmod 4$, and thus $\jmath \in C_1(n)^{\perp}$ and all vectors in $C_1(n)$ have even weight. We need thus only show that there are no vectors of weight 2. Suppose that $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} \in C_1(n)$. Considering cases, and with $w(a)$ as in Eq. (11):

- if $\{a,b,c\} \cap \{d,e,f\} = \emptyset$ then $(w(a), w) = 1$;
- if $\{a,b,c\} \cap \{d,e,f\} = \{a\}$ where $a = d$, then $(w(b), w) = 1$;
- if $\{a,b,c\} \cap \{d,e,f\} = \{a,b\}$ where $a = d, e = b$, then $(w(c), w) = 1$.

This gives a contradiction for all choices of w of weight 2, so the minimum weight is 4.

To show that $C_0(n) = C_1(n)$ for $n \equiv 0 \pmod 4$, we form the sum

$$w = \sum_{\Delta^*} w(\Delta^*)$$

of the words $w(\Delta^*)$ of Eq. (9) over sequences from $\Delta = \{a,b,c,d,e,f\}$ where a,b,c are fixed, and d,e,f vary over the remaining triples, and $w(\Delta^*)$ has $v^{\{a,b,c\}}$ in its support. The number of sets Δ containing a,b,c is $\binom{n-3}{3}$ and each Δ gives nine distinct words $w(\Delta^*)$ with $v^{\{a,b,c\}}$ in the support. In the sum, $v^{\{a,b,c\}}$ will occur $9\binom{n-3}{3} \equiv 0 \pmod 2$ times; each $v^{\{d,e,f\}}$, where $\{d,e,f\}$ is disjoint from $\{a,b,c\}$, will occur $9 \equiv 1 \pmod 2$ times; each $v^{\{a,b,d\}}$, $v^{\{a,c,d\}}$, $v^{\{b,c,d\}}$ will occur once for each $\Delta \ni d$, and thus $\binom{n-4}{2} \equiv 0 \pmod 2$ times. Each $v^{\{a,d,e\}}$, $v^{\{b,d,e\}}$, $v^{\{c,d,e\}}$ will occur once whenever $\{d,e\} \subseteq \Delta$, i.e. $(n-5) \equiv 1 \pmod 2$ times. Thus the sum $w \in C_1(n)$ is

$$\sum_{d,e,f \in \Omega \setminus \{a,b,c\}} v^{\{d,e,f\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{a,d,e\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{b,d,e\}} + \sum_{d,e \in \Omega \setminus \{a,b,c\}} v^{\{c,d,e\}},$$

i.e.

$$w = \sum_{\Delta^*} w(\Delta^*) = v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_1},$$

which shows that $C_0(n) \subseteq C_1(n)$, and, since $C_1(n) \subseteq C_0(n)$ for $n \equiv 0 \pmod 4$ by Lemma 1(1a), hence they are equal.

In the case $n \equiv 1 \pmod 4$, looking at the vector w above, all the congruences modulo 2 remain the same apart from $n-5 \equiv 0 \pmod 2$. Thus we get

$$w = \sum_{\Delta^*} w(\Delta^*) = v^{\overline{\{a,b,c\}}_0}$$

and hence $C_0(n) \subseteq C_1(n)$. Now by Lemma 1(3b), $\jmath \in C_1(n)$, and by Proposition 1, $\jmath \in C_2(n)^\perp$ and hence not in $C_2(n)$, and thus not in $C_0(n)$, since by Lemma 2 $C_0(n) \subseteq C_2(n)$. Thus the containment is proper. □

Lemma 6. *If $w(a)$ is defined as in Eq.* (11), *then the full weight enumerator for*

$$S = \langle \jmath + w(a) \mid a \in \Omega \rangle$$

for $n \equiv 1 \pmod 4 \geqslant 9$ is given as follows: for $r = 1$ to $(n-1)/2$, S has $\binom{n}{r}$ vectors of weight

(1) $r\binom{n-r}{2} + \binom{r}{3}$ *if r is even;*
(2) $\binom{n}{3} - r\binom{n-r}{2} - \binom{r}{3}$ *if r is odd.*

The words have the form $\sum_{i=1}^{r} (\jmath + w(a_i))$ where $\Delta = \{a_1, a_2, \ldots, a_r\}$ has size r. The minimum weight of S is $2\binom{n-2}{2}$ for $n > 9$, and 38 for $n = 9$.

Proof. For Δ as in the statement of the lemma, consider

$$w = \sum_{i=1}^{r} (\jmath + w(a_i)) = r\jmath + \sum_{i=1}^{r} \sum_{x,y \neq a_i} v^{\{a_i,x,y\}}$$

$$= r\jmath + \sum_{i=1}^{r} \left(\sum_{x,y \in \Omega \setminus \Delta} v^{\{a_i,x,y\}} + \sum_{j \neq i} \sum_{x \in \Omega \setminus \Delta} v^{\{a_i,a_j,x\}} + \sum_{j,k \neq i} v^{\{a_i,a_j,a_k\}} \right)$$

$$= r\jmath + \sum_{i=1}^{r} \sum_{x,y \in \Omega \setminus \Delta} v^{\{a_i,x,y\}} + 0 + 3 \sum_{a_i,a_j,a_k \in \Delta} v^{\{a_i,a_j,a_k\}}.$$

The formulae given now follow, where $\binom{r}{3} = 0$ if $r = 1$ or 2.

The smallest weight occurs when $r = 2$ except when $n = 9$ when it occurs at $r = 3$. □

Lemma 7. *For $n \equiv 0 \pmod 4 \geqslant 8$*

$$T = \langle w(a) \mid a \in \Omega \rangle \subseteq C_1(n)^\perp$$

and has weight enumerator as given in Lemma 6 together with the complements of all the words. T is a $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ code.

Proof. The proof is clear from Lemmas 6 and 4. □

Lemma 8. *If $D = \langle u(\Delta^*) \mid \Delta \subset \Omega \rangle$, where $u(\Delta^*)$ is given in Eq.* (10), *then D has dimension at least $\binom{n}{3} - n$.*

Proof. We order the points of $\mathscr{P}$ and a specific set of the words $u(\Delta^*)$ so that the generating matrix is in upper triangular form. The point order is as follows: $\{1,2,3\}, \{1,2,4\}, \ldots, \{1,2,n\}, \{1,3,4\}, \ldots, \{1,3,n\}, \ldots, \{1,n-2,n\}, \{2,3,4\}, \ldots, \{2,n-$

$2, n\}, \ldots, \{n-4, n-2, n-1\}, \{n-4, n-2, n\}$, giving $\binom{n}{3} - n$ positions, followed by the remaining n points: $\{1, n-1, n\}, \{2, n-1, n\}, \ldots, \{n-4, n-1, n\}, \{n-3, n-1, n\}, \{n-2, n-1, n\}, \{n-3, n-2, n-1\}, \{n-3, n-2, n\}$.

The words $u(\Delta^*)$ are ordered according to sequences of elements of Ω of five elements, and writing here, for simplicity, the sequence $[a,b,c,d,e]$ to denote the word $u([a,b,c,d,e]) = v^{\overline{\{a,b,c\}}} + v^{\overline{\{a,b,d\}}} + v^{\overline{\{a,c,e\}}} + v^{\overline{\{a,d,e\}}}$. The ordering is as follows: $[1,2,3,n-1,n], \ldots, [1,2,n-2,n-1,n], [n-1,1,2,n,n-2], [n,1,2,n-1,n-2], \ldots, [1,n-3,n-2,n-1,n], [n-1,1,n-3,n,n-2], [n,1,n-3,n-1,n-2], [n-1,1,n-2,n,n-3], [n,1,n-2,n-1,n-3]$ giving the first $\binom{n-1}{2} - 1$ vectors; $[2,3,4,n-1,n], \ldots [n,2,n-2,n-1,n-3]$ giving the next $\binom{n-2}{2} - 1$ vectors; carry on in this way until $[n-4,n-3,n-2,n-1,n], [n-1,n-4,n-3,n,n-2], [n,n-4,n-3,n-1,n-2], [n-1,n-4,n-2,n,n-3], [n,n-4,n-2,n-1,n-3]$ giving $\binom{n-(n-4)}{2} - 1 = 5$ vectors. The total number of vectors is $\sum_{i=1}^{n-4} (\binom{n-i}{2} - 1) = \binom{n}{3} - n$.

If a matrix of codewords is now formed with the points in the order given, and the rows the words $u(\Delta^*)$ in the order given, then this matrix is in upper triangular form, with $\binom{n}{3} - n$ pivot positions in the first $\binom{n}{3} - n$ positions. Thus D has at least this dimension, for any $n \geqslant 7$. □

Proposition 2. (1) *For* $n \equiv 0 \pmod 4 \geqslant 8$, $C_0(n) = C_1(n)$ *is a* $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ *code, and* $C_0(n)^\perp = C_1(n)^\perp$ *is a* $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ *code with weight enumerator given in Lemma* 7.

(2) *For* $n \equiv 1 \pmod 4 \geqslant 13$, $C_1(n)$ *is a* $[\binom{n}{3}, \binom{n}{3} - n + 1, 4]_2$ *code, and* $C_1(n)^\perp$ *is a* $[\binom{n}{3}, n-1, 2\binom{n-2}{2}]_2$ *code with weight enumerator given in Lemma* 6. *For* $n = 9$, $C_1(9)$ *is a* $[84, 76, 3]_2$ *code and* $C_1(9)^\perp$ *is a* $[84, 8, 38]_2$ *code.*

For all $n \geqslant 7$, $C_1(n) \cap C_1(n)^\perp = \{0\}$. *For* $n \equiv 0 \pmod 4$ *or* $n \equiv 1 \pmod 4$, $\mathrm{Aut}(C_1(n)) = S_n$, *and for* $n \equiv 2 \pmod 4$ *or* $n \equiv 3 \pmod 4$, $\mathrm{Aut}(C_1(n)) = S_{\binom{n}{3}}$.

Proof. First take $n \equiv 0 \pmod 4$. Then by Lemma 7, $C_1(n)^\perp$ has dimension at least n, so $C_1(n)$ has dimension at most $\binom{n}{3} - n$. From Lemma 8, we have $D \subset C_1(n)$ of dimension at least $\binom{n}{3} - n$, and thus equality holds. The facts about the minimum weight of $C_1(n)$ and its dual then follow from Lemmas 5 and 7. That $C_1(n) = C_0(n)$ was proved in Lemma 5.

Now take $n \equiv 1 \pmod 4$. Then $\jmath \in C_1(n)$ but $\jmath \notin C_1(n)^\perp$. Clearly $\jmath \in D^\perp$, and so $D^\perp \supset C_1(n)^\perp$, and $D \subset C_1(n)$. Now $\dim(C_1(n)^\perp) \geqslant \dim(S) = n-1$, and so $\dim(C_1(n)) \leqslant \binom{n}{3} - n + 1$. Since $\dim(D) \geqslant \binom{n}{3} - n$, we have $\dim(C_1(n)) = \binom{n}{3} - n + 1$ and $C_1(n) = \langle D, \jmath \rangle$. This establishes the dimension of the code.

We have already noted the minimum weight of the dual code, since we have just proved that $S = C_1(n)^\perp$ and we can thus use Lemma 6. We need to show that the minimum weight of $C_1(n)$ is 4 unless $n = 9$, in which case we will show that it is 3. Suppose first that $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} \in C_1(n)$. Then $(w, \jmath + w(i)) = 0$ for all $i \in \Omega$. Notice that $\jmath + w(i) = \jmath + \sum_{x,y \neq i} v^{\{i,x,y\}} = \sum_{x,y,z \neq i} v^{\{x,y,z\}}$. Since w is to have weight 2, there is some element a, say, not in $\{d,e,f\}$. Then $(w, \jmath + w(a)) = 1$, giving a contradiction. So there are no elements of weight 2.

Suppose $w = v^{\{a,b,c\}} + v^{\{d,e,f\}} + v^{\{g,h,i\}} \in C_1(n)$. If there is some element $j \in \Omega$ such that $j \notin \{a,b,c,d,e,f,g,h,i\}$, then $(w, \jmath + w(i)) = 3$ and we have a contradiction. This shows that 4 is the minimum weight if $n > 9$. Consider now the case $n = 9$. We show that if $\Omega = \{a,b,c,d,e,f,g,h,i\}$, then $w \in C_1(9)$. Recall from Lemma 1(3b), that $w_P = v^{\{a,b,c\}} + v^{\overline{\{a,b,c\}}_0} + v^{\overline{\{a,b,c\}}_2}$ where w_P is the sum of all the incidence vectors of blocks of $\mathscr{D}_1(n)$ containing the point $P = \{a,b,c\}$. If we form the vector $u = w_{\{a,b,c\}} + w_{\{d,e,f\}} + w_{\{g,h,i\}}$, it is quite direct to show that $u = w$. Thus the minimum weight is 3 when $n = 9$.

Now we show that $C_1(n) + C_1(n)^\perp = F^{\mathscr{P}}$ for each of $n \equiv 0 \pmod 4$ and $n \equiv 1 \pmod 4$ since it already follows for other n. For this, let $P = \{a,b,c\}$ be any point and consider $w = w(a) + w(b) + w(c) + v^{\overline{\{a,b,c\}}_1} \in C_1(n) + C_1(n)^\perp$ for $n \equiv 0 \pmod 4$, and $u = (\jmath + w(a)) + (\jmath + w(b)) + (\jmath + w(c)) + (\jmath + v^{\overline{\{a,b,c\}}_1}) \in C_1(n) + C_1(n)^\perp$ for $n \equiv 1 \pmod 4$. It is immediate that $w = u = v^{\{a,b,c\}}$, which establishes the result.

To prove the stated results about the automorphism groups, if $n \equiv 0 \pmod 4$, then by Lemma 4, $\{w(a) \mid a \in \Omega\}$ is the set of words of weight $\binom{n-1}{2}$ in $C_1(n)^\perp$. Hence if $\alpha \in \mathrm{Aut}(C_1(n)^\perp)$, then $\alpha(w(a)) = w(b)$ and since $w(a) = w(b)$ if and only if $a = b$, we deduce that α is defined in S_n and hence $\mathrm{Aut}(C_1(n)) = S_n$.

Now assume that $n \equiv 1 \pmod 4$. Then for $n \geqslant 13$, $C_1(n)^\perp$ has minimum weight $2\binom{n-1}{2}$. The set

$$\{j + w(a) + j + w(b) \mid a, b \in \Omega, a \neq b\} = \{w(a) + w(b) \mid a, b \in \Omega, a \neq b\}$$

is the set of all vectors of minimum weight (this follows from Lemma 6 and the fact that $S = C_1(n)^\perp$). Using the definition of $w(a)$, it is easy to see that

$$w(a) + w(b) = \sum_{x,y \in \Omega \setminus \{a,b\}} (v^{\{a,x,y\}} + v^{\{b,x,y\}}).$$

Now it is clear that $w(a) + w(b) = w(c) + w(d)$ if and only if $\{a,b\} = \{c,d\}$. So we deduce that if $\alpha \in \mathrm{Aut}(C_1(n))$, then α maps pairs to pairs. Now the proof follows similarly to the proof in Proposition 1. For $n = 9$, direct computations with MAGMA show that $\mathrm{Aut}(C_1(9)) = S_9$.

For $n \equiv 2 \pmod 4$, $C_1(n) = F_2^{\binom{n}{3}}$ and hence the result. For $n \equiv 3 \pmod 4$, we can easily see that $\mathrm{Aut}(C_1(n)) = S_{\binom{n}{3}}$, because $C_1(n) = \langle v^P + \jmath \mid P \in \mathscr{P} \rangle$ and for any $g \in S_{\binom{n}{3}}$ we have $g(v^P + \jmath) = v^Q + \jmath$. □

Lemma 9. *For* $n \equiv 1 \pmod 4$, $C_1(n) + C_2(n) = F_2^{\mathscr{P}}$ *and* $C_2(n)^{\perp} \cap T = \langle \jmath \rangle$ *where* T *is as defined in Lemma* 7.

Proof. From Lemma 1(3b), we have $v^{\{a,b,c\}} = w_{\{a,b,c\}} + u$, where $w_{\{a,b,c\}} \in C_1(n)$ and $u \in C_2(n)$, since $C_0(n) \subseteq C_2(n)$ by Lemma 2, and thus $C_1(n) + C_2(n) = F_2^{\mathscr{P}}$. It follows that $C_1(n)^{\perp} \cap C_2(n)^{\perp} = \{0\}$, i.e. $S \cap C_2(n)^{\perp} = \{0\}$, where S is defined in Lemma 4. Suppose that $u \in C_2(n)^{\perp} \cap T$. Then $u = \sum_a w(a)$. Either $u = \sum_a (\jmath + w(a))$ or $u + \jmath = \sum_a (\jmath + w(a))$. Recalling that $\jmath \in C_2(n)^{\perp}$, we see that either $u = 0$ or $u = \jmath$, which proves the assertion. □

Note: From Lemma 9 and earlier results we see that, for $n \equiv 1 \pmod 4$,

(1) $C_0(n) \subset C_2(n)$;
(2) $C_0(n) \subseteq C_1(n) \cap C_2(n)$;
(3) $\dim(C_0(n)) \leqslant \binom{n}{3} - \binom{n}{2}$.

Lemma 10. *If* $E = \langle w(\pi) \mid \pi \rangle$ *where* $w(\pi)$ *is defined in Eq.* (8) *and* π *ranges over all partitions of all six-element subsets* Δ *of* Ω, *then* $\dim(E) \geqslant \binom{n}{3} - \binom{n}{2}$.

If $n \equiv 1 \pmod 4$, $C_0(n) = E$ *and has dimension* $\binom{n}{3} - \binom{n}{2}$. *Furthermore*, $C_0(n) = C_1(n) \cap C_2(n)$.

Proof. The proof follows similar ideas to those in Lemma 8. Thus we order the points of $\mathscr{P}$ and a specific set of the words $w(\pi)$ so that the generating matrix is in upper triangular form. The point order is as follows: $\{1,2,3\}, \{1,2,4\}, \ldots, \{1,2,n-1\}, \{1,3,4\}, \ldots, \{1,3,n-1\}, \ldots, \{1,n-3,n-2\}, \{1,n-3,n-1\}, \{2,3,4\}, \ldots, \{2,n-3,n-1\}, \ldots, \{n-5,n-3,n-2\}, \{n-5,n-3,n-1\}$, giving $\binom{n}{3} - \binom{n}{2}$ positions, followed by the remaining points in arbitrary order.

The words $w(\pi)$ are ordered according to partitions of subsets of Ω of six elements; write here, for simplicity, the sequence $[a,b,c,d,e,f]$ to denote the word $w(\pi)$ with partition $\pi = \{\{a,b\},\{c,d\},\{e,f\}\}$. Thus $w(\pi)$ is the vector

$$v^{\{a,c,e\}} + v^{\{a,c,f\}} + v^{\{a,d,e\}} + v^{\{a,d,f\}} + v^{\{b,c,e\}} + v^{\{b,c,f\}} + v^{\{b,d,e\}} + v^{\{b,d,f\}}.$$

We will refer to the term in the support of $w(\pi)$ that is earliest in the ordering of the points as given above, as the leading term of $w(\pi)$. We will choose our π so that the leading terms will be the pivot positions in the generating matrix.

Using this notation the ordering is as follows: $[1,n-2,2,n-1,3,n], [1,n-2,2,n-1,4,n], \ldots, [1,n-2,2,n-1,n-3,n], [1,n-3,2,n-1,n-2,n], [1,n-3,2,n-2,n-1,n], [1,n-2,3,n-1,4,n], \ldots, [1,n-3,3,n-2,n-1,n], \ldots, [1,n-3,n-4,n-2,n-1,n]$ and $[1,n-4,n-3,n-1,n-2,n], [1,n-4,n-3,n-2,n-1,n]$ for the first $\binom{n-2}{2} - 1$ vectors, with leading terms the points $\{1,2,3\}, \ldots, \{1,n-3,n-1\}$. The next vectors are $[2,n-2,3,n-1,4,n], \ldots, [2,n-4,n-3,n-2,n-1,n]$ giving another $\binom{n-3}{2} - 1$ vectors with leading terms the points $\{2,3,4\}, \ldots, \{2,n-3,n-1\}$. Continue in this way up to the last set of five vectors: $[n-5,n-2,n-4,n-1,n-3,n], [n-5,n-3,n-4,n-1,n-2,n], [n-5,n-3,n-4,n-2,n-1,n], [n-5,n-4,n-3,n-1,n-2,n], [n-5,n-4,n-3,n-2,n-1,n]$, with leading terms $\{n-5,n-4,n-3\}, \{n-5,n-4,n-2\}, \{n-5,n-4,n-1\}, \{n-5,n-3,n-2\}, \{n-5,n-3,n-1\}$. The number of terms is the sum of these which is again easily seen to be $\binom{n}{3} - \binom{n}{2}$.

If a matrix of codewords is now formed with the points in the order given, and the rows the words $w(\pi)$ in the order given, then this matrix is in upper triangular form, with $\binom{n}{3} - \binom{n}{2}$ pivot positions in the first $\binom{n}{3} - \binom{n}{2}$ positions. Thus E has at least this dimension, for any $n \geqslant 7$.

If $n \equiv 1 \pmod 4$, then $\dim(C_0(n)) \leqslant \binom{n}{3} - \binom{n}{2}$, as noted above. Since $E \subseteq C_0(n)$, we have equality, and since this is also the dimension of $C_1(n) \cap C_2(n)$, this completes the proof. □

Note: In the appendix we show the ordering of the vectors in the case $n = 9$.

Proposition 3. *For* $n \equiv 1 \pmod 4 \geqslant 9$, $C_0(n)$ *is a* $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ *code, and* $C_0(n)^{\perp}$ *is a* $[\binom{n}{3}, \binom{n}{2}, n-2]_2$ *code. Further*, $C_0(n) \cap C_0(n)^{\perp} = \{0\}$.

For $n \not\equiv 2 \pmod 4$, $\mathrm{Aut}(C_0(n)) = S_n$ *and for* $n \equiv 2 \pmod 4$, $\mathrm{Aut}(C_0(n)) = S_{\binom{n}{3}}$.

Proof. Since $C_0(n) \subset C_2(n)$, its minimum weight is at least 4, and a vector of weight 4 would be of the form $w(a,b,c,d) \in C_2(n)$, as shown in Proposition 1. Since these words span $C_2(n)$ and since $\mathrm{Aut}(C_0(n)) \supseteq S_n$, which is transitive on 4-tuples, if $C_0(n)$ contained one word of weight 4 it would contain all those in $C_2(n)$ and hence $C_0(n) = C_2(n)$, which is a contradiction for $n \equiv 1 \pmod 4$. Thus its minimum weight is 6 or 8. If it contained a word of weight 6 then such a word would be in both $C_2(n)$ and $C_1(n)$, and $w = w(a,b,c,d) + w(a,b,c,e)$ would be a candidate. Consider the vector $u = u([a,b,d,e,c]) = v^{\{a,b,d\}} + v^{\{a,b,e\}} + v^{\{a,d,c\}} + v^{\{a,e,c\}} \in C_1(n)$. Then $w + u \in C_1(n)$ and has weight 2, which is a contradiction. Thus we need only show that the words of weight 6 in $C_2(n)$ have the form of w, in which case it will follow that $C_0(n)$ will have minimum weight 8. For this, we use the words $w(a,b) \in C_2(n)^{\perp}$, as defined in Eq. (7). Suppose u is a word of weight 6 in $C_2(n)$. Any $w(a,b)$ must meet the support of u evenly: clearly six times is impossible, since if $\{a,b,c\}$ is in the support, then $(w(b,c),u) = 1$. Four times is also easily seen to be impossible for the same reason, so any $w(a,b)$ can meet the support of u twice or not at all. Thus u must be such that if $\{a,b,c\}$ is in its support, each pair $\{a,b\}$, $\{a,c\}$ and $\{b,c\}$ must occur again in a point in the support of u. Consideration of the possibilities leads only to a word of the form $w = w(a,b,c,d) + w(a,b,c,e)$. Thus the minimum weight of $C_0(n)$ is 8. That the minimum weight of $C_0(n)^{\perp}$ is $n-2$ follows by a similar argument to that given in Proposition 1.

To show that $C_0(n) \cap C_0(n)^{\perp} = \{0\}$, again we show that $C_0(n) + C_0(n)^{\perp} = F_2^{\mathscr{P}}$. Recall that $w(a)$ and $w(a,b)$ are in $C_0(n)^{\perp}$, where $w(a)$ is as defined in Eq. (11). Then, for any $\{a,b,c\}$, $w(a)+w(b)+w(c)+w(a,b)+w(a,c)+w(b,c)+\jmath + v^{\overline{\{a,b,c\}}_0} = (w(a)+w(b)+w(c)+v^{\overline{\{a,b,c\}}_1}) + (w(a,b)+w(a,c)+w(b,c)+v^{\overline{\{a,b,c\}}_2}) + v^{\{a,b,c\}} = v^{\{a,b,c\}}$, as we observed before (and using Eq. (4)) and hence $C_0(n) + C_0(n)^{\perp} = F_2^{\mathscr{P}}$.

For the automorphism groups, if $n \equiv 0 \pmod 4$, then $C_0(n) = C_1(n)$ and hence $\mathrm{Aut}(C_0(n)) = \mathrm{Aut}(C_1(n)) = S_n$ by Proposition 2. If $n \equiv 1 \pmod 4$, then by Lemma 6, $\{w(a) \mid a \in \Omega\}$ is the set of words of weight $\binom{n-1}{2}$ for $C_0(n)^{\perp}$. Now the proof is similar to the proof in Proposition 2. If $n \equiv 3 \pmod 4$, then $C_0(n) = C_2(n)$ and the result follows from Proposition 1. For $n \equiv 2 \pmod 4$, $C_2(n) = F_2^{\mathscr{P}}$ and the result follows. □

Appendix A

The table below shows the ordering of the vectors $w(\pi)$ as given in Lemma 10, in the case $n = 9$. Read down the successive columns. The leading terms, corresponding to pivot positions, can be read from the first, third and fifth elements in each block: thus the block [1 7 2 8 5 9] has leading term $\{1,2,5\}$.

1 7 2 8 3 9	2 7 3 8 4 9	3 7 4 8 5 9
1 7 2 8 4 9	2 7 3 8 5 9	3 7 4 8 6 9
1 7 2 8 5 9	2 7 3 8 6 9	3 6 4 8 7 9
1 7 2 8 6 9	2 6 3 8 7 9	3 6 4 7 8 9
1 6 2 8 7 9	2 6 3 7 8 9	3 7 5 8 6 9
1 6 2 7 8 9	2 7 4 8 5 9	3 6 5 8 7 9
1 7 3 8 4 9	2 7 4 8 6 9	3 6 5 7 8 9
1 7 3 8 5 9	2 6 4 8 7 9	3 5 6 8 7 9
1 7 3 8 6 9	2 6 4 7 8 9	3 5 6 7 8 9
1 6 3 8 7 9	2 7 5 8 6 9	4 7 5 8 6 9
1 6 3 7 8 9	2 6 5 8 7 9	4 6 5 8 7 9
1 7 4 8 5 9	2 6 5 7 8 9	4 6 5 7 8 9
1 7 4 8 6 9	2 5 6 8 7 9	4 5 6 8 7 9
1 6 4 8 7 9	2 5 6 7 8 9	4 5 6 7 8 9
1 6 4 7 8 9		
1 7 5 8 6 9		
1 6 5 8 7 9		
1 6 5 7 8 9		
1 5 6 8 7 9		
1 5 6 7 8 9		

References

[1] E.F. Assmus, Jr., J.D. Key, Designs and their Codes, Cambridge Tracts in Mathematics, Vol. 103, Cambridge University Press, Cambridge, 1992 (Second printing with corrections, 1993).

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

[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, November 1994. http://www.maths.usyd.edu.au:8000/u/magma/

[4] A.E. Brouwer, C.J. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, J. Algebraic Combin. 1 (1992) 329–346.

[5] A.E. Brouwer, J.H. van Lint, Strongly regular graphs and partial geometries, in: D.M. Jackson, S.A. Vanstone (Eds.), Enumeration and Design, Academic Press, Toronto, 1984, pp. 85–122. Proceedings of the Silver Jubilee Conference on Combinatorics, Waterloo, 1982.

[6] W.H. Haemers, R. Peeters, J.M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr. 17 (1999) 187–209.

[7] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman, (Eds.), Handbook of Coding Theory, Vol. 2, Part 2. Elsevier, Amsterdam, 1998, pp. 1345–1440. (Chapter 17).

[8] J.D. Key, J. Moori, B.G. Rodrigues, Permutation decoding for binary codes from triangular graphs, European J. Combin. 25 (2004) 113–123.

[9] J.D. Key, J. Moori, B.G. Rodrigues, Permutation decoding of binary codes from graphs on triples, submitted.

[10] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.

[11] V.D. Tonchev, Combinatorial Configurations, Designs, Codes, Graphs, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 40. Longman, New York, 1988 (Translated from Bulgarian by Robert A. Melter).