Codes associated with triangular graphs, and permutation decoding

J. D. Key and J. Moori[*]
School of Mathematical Sciences
University of KwaZulu-Natal
Pietermaritzburg 3209, South Africa

B. G. Rodrigues
School of Mathematical Sciences
University of KwaZulu-Natal
Durban 4041, South Africa

March 17, 2009

Abstract

Non-binary linear codes of length $\binom{n}{2}$, dimension n or $n-1$, minimum weight $n-1$ or $2n-4$, respectively, that can be obtained from designs associated with the complete graph on n vertices and their line graphs, the triangular graphs, are examined. The parameters of the codes and their automorphism groups for any odd prime are obtained and PD-sets inside the symmetric group S_n are found for full permutation decoding for all primes and all integers $n \geq 6$.

1 Introduction

For any n the triangular graph is defined to be the line graph of the complete graph K_n. It is a strongly regular graph on $v = \binom{n}{2}$ vertices. The binary codes from the span of adjacency matrices of triangular graphs have been examined by various authors: see [3, 4, 8, 18], and with a view to permutation decoding in [6, 11, 16]. Here we examine the p-ary codes for odd primes p; the p-rank of these and related graphs was examined in [15]. Considering the triangular graph T_n as a uniform-subset graph with vertices the 2-subsets of $\Omega = \{1, \ldots, n\}$, and adjacency defined by $\{a, b\}$ adjacent to $\{c, d\}$ if and only if c or d, but not both, is equal to a or b, if A_n denotes an adjacency matrix for T_n then $B_n = J - I - A_n$, where J is the all-one and I the identity $\binom{n}{2} \times \binom{n}{2}$ matrix, will be an adjacency matrix for the the graph $\widetilde{T}_n$ on the same vertices with adjacency defined by $\{a, b\}$ adjacent to $\{c, d\}$ if $\{a, b\} \cap \{c, d\} = \emptyset$. We examine the neighbourhood designs and p-ary codes, for any odd prime p, from A_n, $A_n + I$, B_n, $B_n + I$ and show that all the codes are inside the code or its dual obtained from an incidence matrix M_n for the complete graph K_n. Thus the latter codes, and some subcodes of codimension 1, are the ones that we examine for permutation decoding. Note that $A_n + I$ and $B_n + I$ are adjacency matrices for the graphs T_n^R and $\widetilde{T}_n^R$ obtained from T_n and $\widetilde{T}_n$, respectively, by including all loops, and thus referred to as reflexive graphs.

We summarize our results below in a theorem; the specific results relating to the codes from $T_n, \tilde{T}_n, T_n^R, \tilde{T}_n^R$ are given as propositions and lemmas in the following sections.

Theorem 1 *Let C_n be the p-ary code of an incidence matrix M_n for the complete graph K_n where p is any odd prime and $n \geq 5$. Then C_n is a $[\binom{n}{2}, n, n-1]_p$ code with information set*

$$\mathcal{I}_n = \{\{1, n\}, \ldots, \{n-1, n\}, \{1, 2\}\},$$

[*] Support of NRF and the University of KwaZulu-Natal acknowledged.

where $\{i,j\}$ denotes the edge of K_n between the vertices $i,j \in \Omega$.

For $n \geq 6$ the minimum words of C_n are the scalar multiples of the rows of M_n, and $\mathrm{Aut}(C_n) = S_n$. The set

$$S = \{(n,i)(1,j) \mid 1 \leq i \leq n, 1 \leq j \leq n-1\}$$

of elements of S_n, where $(i,j) \in S_n$ is a transposition and (k,k) is the identity of S_n, is a PD-set of size $n(n-1)$ for C_n for the information set $\mathcal{I}_n$. For $n \geq 8$, C_n has no words of weight d in the range $n \leq d \leq 2n-5$.

Let $E_n = \langle r_i - r_j \mid r_i, r_j$ rows of $M_n \rangle$. Then for $n \geq 8$, E_n is an $[\binom{n}{2}, n-1, 2n-4]_p$ code. For $n \geq 4$, $\mathcal{I}_n^* = \mathcal{I}_n \setminus \{\{n-1,n\}\}$ is an information set for E_n. For $n \geq 9$, the minimum words of E_n are the scalar multiples of $r_i - r_j$, $1 \leq i,j \leq n$, where r_i, r_j are rows of M_n.

For $n \geq 7$,

$$S^* = \{(n-1,i)(n,j)(1,k) \mid 1 \leq i \leq n-1, 1 \leq j \leq n, 3 \leq k \leq n-1\},$$

is a PD-set of size $n(n^2-5n+7)$ for E_n for the information set $\mathcal{I}_n^*$.

The p-ary codes from $T_n, \widetilde{T}_n, T_n^R, \widetilde{T}_n^R$ are either $\mathbb{F}_p^{\binom{n}{2}}$, $\langle \boldsymbol{\jmath} \rangle^\perp$, $C_n^\perp$ or $E_n^\perp$, where $\boldsymbol{\jmath}$ is the all-one vector.

We note that even in the binary case the codes from the triangular graph that are of interest are C_n or E_n: see Result 1 in Section 2. The binary codes from $\widetilde{T}_n$ have been studied by Fish [6].

The proof of the theorem follows from propositions and lemmas in the following sections. The full details about the codes from $T_n, \widetilde{T}_n, T_n^R, \widetilde{T}_n^R$ are in Proposition 7. Background definitions are given in Section 2, and notation for the graphs, designs and codes that we consider here is given in Section 3.

2 Background and terminology

The notation for designs and codes is as in [1]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{J})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{J}$ is a t-(v,k,λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is **symmetric** if it has the same number of points and blocks. The **code $\boldsymbol{C_F(\mathcal{D})}$ of the design** $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the **incidence vector** of $\mathcal{Q}$ by $\boldsymbol{v^{\mathcal{Q}}}$, and if $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$, then we will write v^P instead of $v^{\{P\}}$. Thus $C_F(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any $w \in F^{\mathcal{P}}$ and $P \in \mathcal{P}$, $\boldsymbol{w(P)}$ denotes the value of w at P. If $F = \mathbb{F}_p$ then the **$\boldsymbol{p}$-rank** of the design, written $\mathrm{rank}_{\boldsymbol{p}}\boldsymbol{(\mathcal{D})}$, is the dimension of its code $C_F(\mathcal{D})$, which we usually write as $C_p(\mathcal{D})$.

All the codes here are **linear codes**, and the notation $[n,k,d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight $\mathbf{wt}(\boldsymbol{v})$** of a vector v is the number of non-zero coordinate entries. The **distance $\mathbf{d}(\boldsymbol{u},\boldsymbol{v})$** between two vectors u, v is the number of coordinate positions in which they differ, i.e., $\mathrm{wt}(u-v)$. A **generator matrix** for C is a $k \times n$ matrix made up of a basis for C, and the **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n | (v,c) = 0 \text{ for all } c \in C\}$. If $C = C_p(\mathcal{D})$, where $\mathcal{D}$ is a design, then $C \cap C^\perp$ is the **hull** of $\mathcal{D}$ at p, or simply the **hull** of $\mathcal{D}$ or C if p and $\mathcal{D}$ are clear from the context. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the vector with all entries equal to 1. Two linear codes of the same length and over the same field 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 code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \,|\, A]$; a check matrix then is given by $[-A^T \,|\, I_{n-k}]$. The set of the first k coordinates in the standard form is called an **information set** for the code, and the set of the last $n-k$ coordinates is the corresponding **check set**.

The **graphs**, $\Gamma = (V, E)$ with vertex set V and edge set E, discussed here are undirected with no loops, apart from the case where **all** loops are included, in which case the graph is called **reflexive**. A graph is **regular** if all the vertices have the same valency. An **adjacency matrix** A of a graph of order n is an $n \times n$ matrix with entries a_{ij} such that $a_{ij} = 1$ if vertices v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. An **incidence matrix** of Γ is an $n \times |E|$ matrix B with $b_{i,j} = 1$ if the vertex labelled by i is on the edge labelled by j, and $b_{i,j} = 0$ otherwise. If Γ is regular with valency k, then the 1-$(|E|, k, 2)$ design with incidence matrix B is called the **incidence design** of Γ. The **neighbourhood design** of a regular graph is the 1-design formed by taking the points to be the vertices of the graph and the blocks to be the sets of neighbours of a vertex, for each vertex, i.e. an adjacency matrix as an incidence matrix for the design. The **line graph** of a graph $\Gamma = (V, E)$ is the graph $L(\Gamma) = (E, V)$ where e and f are adjacent in $L(\Gamma)$ if e and f share a vertex in Γ. The **code** of a graph Γ over a finite field F is the row span of an adjacency matrix A over the field F, denoted by $C_F(\Gamma)$ or $C_F(A)$. The dimension of the code is the rank of the matrix over F, also written $\mathrm{rank}_p(A)$ if $F = \mathbb{F}_p$, in which case we will speak of the p**-rank** of A or Γ, and write $C_p(\Gamma)$ or $C_p(A)$ for the code.

Permutation decoding, first developed by MacWilliams [13], involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [14, Chapter 16, p. 513] and Huffman [9, Section 8]. In [10] and [12] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1 *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

*For $s \leq t$ an s-***PD-set** *is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is given in [9] and requires that the generator matrix is in standard form. Furthermore, there is a bound on the minimum size of $\mathcal{S}$ (see [7],[17], or [9]).

We are studying here p-ary codes, for odd p, related to the triangular graphs. The analogous result in the binary case can be found in [11], in which the main result was as follows:

Result 1 *For $n \geq 5$, T_n the triangular graph, and $C = C_2(T_n)$ with the vertices*

$$\mathcal{I} = \{\{1, n\}, \{2, n\}, \ldots, \{n-1, n\}\}$$

in the first $n-1$ positions:

1. *C is an $[\binom{n}{2}, n-1, n-1]_2$ code for n odd and, with $\mathcal{I}$ as the information set, $\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\}$ is a PD-set for C of n elements in S_n;*

2. *C is an $[\binom{n}{2}, n-2, 2(n-2)]_2$ code for n even, and with $\mathcal{I}$ excluding $\{n-1, n\}$ as the information set, $\mathcal{S} = \{1_G\} \cup \{(i,n) \mid 1 \leq i \leq n-1\} \cup \{[(i,n-1)(j,n)]^{\pm 1} \mid 1 \leq i,j \leq n-2\}$ is a PD-set for C of $n^2 - 2n + 2$ elements in S_n.*

Note that there is a typographical error in this statement in [11], where the minimum weight in the even case is stated as $2(n-1)$ in Theorem 1.1 of that paper. The code C in the result is the code C_n of Theorem 1 for $p = 2$ and n odd, and E_n for n even.

3 The graphs, designs and codes

In all the following, p is an **odd** prime, and $n \geq 3$. Many of the results hold in some way for the binary codes as well, but since these codes have already been studied elsewhere, we will not include comments on this case. We now set up our notation for the graphs, designs and codes that we will be examining.

For any $n \geq 3$, let $\mathcal{G}_n$ denote the incidence design of the complete graph K_n. Thus $\mathcal{G}_n$ is a 1-$(\binom{n}{2}, n-1, 2)$ design. The point set of $\mathcal{G}_n$ will be denoted by $\mathcal{P}_n$ and will be the same for all the classes of designs here. Writing $\Omega = \{1, \ldots, n\}$, we take for incidence matrix M_n where the rows are labelled by the vertices from Ω, and the columns are labelled inductively from the edges as follows:

$$\{1,2\}, \{1,3\}, \{2,3\}, \{1,4\}, \{2,4\}, \{3,4\}, \ldots, \{1,n\}, \ldots, \{n-1,n\},$$

so that

$$M_n = \left[\begin{array}{cc} M_{n-1} & I_{n-1} \\ 0 \ldots 0 & 1 \ldots 1 \end{array} \right]. \tag{1}$$

For $a \in \Omega$ the block of $\mathcal{G}_n$ defined by the row a will be written as

$$\overline{a} = \{\{a,b\} \mid b \in \Omega \setminus \{a\}\}. \tag{2}$$

Writing $C_p(\mathcal{G}_n) = C_p(M_n) = C_n$, assuming the prime p is clear from the context, then

$$C_n = \langle\ v^{\overline{a}} \mid a \in \Omega \rangle, \tag{3}$$

where the span is taken over $\mathbb{F}_p$. Furthermore

$$E_n = \langle\ v^{\overline{a}} -\ v^{\overline{b}} \mid a, b \in \Omega \rangle. \tag{4}$$

The triangular graph T_n is the line graph $L(K_n)$. The rows of an adjacency matrix A_n for T_n give the blocks of the neighbourhood design of T_n which we will denote by $\overline{\mathcal{D}}_n$. The blocks are

$$\overline{\{a,b\}} = \{\{a,c\} \mid c \neq a, b\} \cup \{\{c,b\} \mid c \neq a, b\} \tag{5}$$

for each point $\{a,b\} \in \mathcal{P}_n$. Thus for $n \geq 5$, $\overline{\mathcal{D}}_n$ is a symmetric 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design. We write

$$\overline{C}_n = \langle\ v^{\overline{\{a,b\}}} \mid \{a,b\} \in \mathcal{P}_n \rangle. \tag{6}$$

For the reflexive triangular graph T_n^R, we get the 1-$(\binom{n}{2}, 2n-3, 2n-3)$ design $\overline{\overline{\mathcal{D}}}_n$ with blocks

$$\overline{\overline{\{a,b\}}} = \{\{a,c\} \mid c \neq a, b\} \cup \{\{c,b\} \mid c \neq a, b\} \cup \{\{a,b\}\} = \ \overline{\{a,b\}} \cup \{\{a,b\}\} \tag{7}$$

for each point $\{a,b\} \in \mathcal{P}_n$, and p-ary code

$$\overline{\overline{C}}_n = \langle\, v^{\overline{\overline{\{a,b\}}}} \mid \{a,b\} \in \mathcal{P}_n \rangle. \tag{8}$$

The graph $\widetilde{T}_n$ where $\{a,b\}$ is adjacent to $\{c,d\}$ if the two 2-subsets do not intersect, gives a symmetric 1-$(\binom{n}{2}, \binom{n-2}{2}, \binom{n-2}{2})$ design $\widetilde{\mathcal{D}}_n$ with blocks

$$\widetilde{\{a,b\}} = \{\{c,d\} \mid \{a,b\} \cap \{c,d\} = \emptyset\} = \mathcal{P}_n \setminus \overline{\overline{\{a,b\}}} \tag{9}$$

for each point $\{a,b\} \in \mathcal{P}_n$, and p-ary code

$$\widetilde{C}_n = \langle\, v^{\widetilde{\{a,b\}}} \mid \{a,b\} \in \mathcal{P}_n \rangle. \tag{10}$$

Finally, from the reflexive graph $\widetilde{T}_n^R$ we get a 1-$(\binom{n}{2}, \binom{n-2}{2}+1, \binom{n-2}{2}+1)$ design $\widetilde{\widetilde{\mathcal{D}}}_n$ with blocks

$$\widetilde{\widetilde{\{a,b\}}} = \{\{c,d\} \mid \{a,b\} \cap \{c,d\} = \emptyset\} \cup \{\{a,b\}\} = \widetilde{\{a,b\}} \cup \{\{a,b\}\} \tag{11}$$

for each point $\{a,b\} \in \mathcal{P}_n$, and p-ary code

$$\widetilde{\widetilde{C}}_n = \langle\, v^{\widetilde{\widetilde{\{a,b\}}}} \mid \{a,b\} \in \mathcal{P}_n \rangle. \tag{12}$$

Note also that if $\boldsymbol{\jmath}$ denotes the all-one vector of length $\binom{n}{2}$, then, for all $\{a,b\} \in \mathcal{P}_n$,

$$v^{\overline{\overline{\{a,b\}}}} + v^{\widetilde{\{a,b\}}} = \boldsymbol{\jmath} = v^{\overline{\{a,b\}}} + v^{\widetilde{\widetilde{\{a,b\}}}}. \tag{13}$$

The symmetric group S_n acts on each of these graphs, designs and codes. We will establish when it is the full automorphism group.

4 Codes from $\mathcal{G}_n$

We establish the basic properties of $C_n = C_p(\mathcal{G}_n) = C_p(M_n)$. The argument works for all odd primes p. For $n = 3$ the codes are of no interest. We first need a lemma. The notation throughout will be as established in the last section.

Lemma 1 *For $n \geq 4$, if $\{a,b,c,d\} \subseteq \Omega$ where a,b,c,d are all distinct, then the vector*

$$u(a,b,c,d) = v^{\{a,b\}} + v^{\{c,d\}} - v^{\{a,c\}} - v^{\{b,d\}} \tag{14}$$

is in $C_n^{\perp}$.

Proof: This is clear since $(\overline{x}, u(a,b,c,d)) = 0$ for all choices of $x \in \Omega$. ■

Proposition 1 *For $n \geq 5$, any odd prime p, C_n is a $[\binom{n}{2}, n, n-1]_p$ code. For $n \geq 6$ the minimum-weight vectors are the scalar multiples of the incidence vectors of the blocks of $\mathcal{G}_n$.*

Proof: We consider the row span over $\mathbb{F}_p$ of the matrix M_n from Equation (1). Clearly $\dim(C_3) = 3$ and by induction it follows that $\dim(M_n) = n$. Each row has weight $n-1$ so the minimum weight cannot be greater than this.

Now let $\mathcal{B}_n$ be the set of supports of the vectors $u(a,b,c,d)$ as defined in Equation (14). Then $(\mathcal{P}_n, \mathcal{B}_n)$ is a 1-$(\binom{n}{2}, 4, r)$ design, where $r = (n-2)(n-3)$. The number of blocks is $3\binom{n}{4}$.

Let $w \in C_n$ and $\text{Supp}(w) = \mathcal{S}$, where $|\mathcal{S}| = s$. Let $P \in \mathcal{S}$. We first count the number of blocks of $\mathcal{B}_n$ through P and another point Q. Suppose $P = \{a,b\}$. Then

1. if $Q = \{a,c\}$ then $P, Q \in \text{Supp}(u(a,b,c,d))$ for all $d \in \Omega \setminus \{a,b,c\}$, giving $n-3$ such blocks;
2. if $Q = \{c,b\}$ then P, Q are on $n-3$ blocks again;
3. if $Q = \{c,d\}$ where $c, d \neq a, b$, then $P, Q \in \text{Supp}(u(a,b,c,d)), \text{Supp}(u(a,b,d,c))$, giving two blocks.

Suppose that in $\mathcal{S}$ there are k points of the type $\{a,c\}$ or $\{b,c\}$, and ℓ of the type $\{c,d\}$ where $c, d \neq a, b$. Then $s = k + \ell + 1$. Counting blocks of $\mathcal{B}_n$ through the point P, suppose that there are z_i that meet $\mathcal{S}$ in i points. Then $z_0 = z_1 = z_i = 0$ for $i \geq 5$, since w cannot meet a block of $\mathcal{B}_n$ only once. Thus $r = z_2 + z_3 + z_4$ and $z_2 + 2z_3 + 3z_4 = (n-3)k + 2\ell = (n-3)(s-\ell-1) + 2\ell$. Thus $r = (n-2)(n-3) \leq (n-3)(s-1) - (n-5)\ell \leq (n-3)(s-1)$ for $n \geq 5$. So $s \geq n-1$ for $n \geq 5$, giving the minimum weight as stated.

Now we show that for $n \geq 6$ the vectors of weight $n-1$ must be scalar multiples of the blocks of $\mathcal{G}_n$. Suppose $s = n-1$ with the same notation as above. Putting $s = n-1$ in the equations above, we get $(n-2)(n-3) \leq z_2 + 2z_3 + 3z_4 = (n-3)(n-2) - (n-5)\ell$. Since $n-5 > 0$ this implies that $\ell = 0$, and $r = z_2 + z_3 + z_4 = z_2 + 2z_3 + 3z_4$. Thus $z_3 = z_4 = 0$, $k = n-2$ and $\mathcal{S} \setminus \{P\}$ consists of at least $n-2 \geq 4$ points and they are all of the form $\{a,c\}$ or $\{b,c\}$. Suppose there are k_1 of the form $\{a,c\}$ and k_2 of the form $\{b,c\}$. If $k_1 = 0$ or $k_2 = 0$ then $\mathcal{S} = \overline{a}$ or $\overline{b}$. If $k_1, k_2 \geq 1$ then either $k_1 \geq 2$ or $k_2 \geq 2$. Suppose $k_1 \geq 2$ and $\{a,c\}, \{a,d\}, \{b,e\} \in \mathcal{S}$. If $e \neq c$ then we can make the same counting argument using the point $\{a,c\}$ for P and get a contradiction for $\ell = 0$. Thus $\mathcal{S} = \overline{a}$, say. If $w \neq \alpha\, v^{\overline{a}}$ for some $\alpha \in \mathbb{F}_p$ then $\text{wt}(w + \beta\, v^{\overline{a}}) < n-1$ for some $\beta \in \mathbb{F}_p$, contradicting the minimum weight being $n-1$. Thus we have our result. ■

Note: For all odd p, if $n = 3$ the minimum weight is 1, and if $n = 4$ it is 2. For $n = 5$ there are words of weight 4 in C_n that are not scalar multiples of the incidence vectors of the blocks of $\mathcal{G}_n$, for example $w = \boldsymbol{\jmath} - v^{\overline{1}} - v^{\overline{2}}$.

Proposition 2 *For $n \geq 4$, $C_n = C_p(\mathcal{G}_n)$ where p is any odd prime, then*

$$\mathcal{U} = \bigcup_{i=1}^{n-3} \{u(i,j,n-1,n) \mid i+1 \leq j \leq n-2\} \cup \{u(i,n-1,n,i+1) \mid 1 \leq i \leq n-3\}$$

is a basis for $C_n^{\perp}$.

Proof: If the matrix M_n from Equation (1) is written in its original recursive form then, with this ordering of the columns (points), we can order the vectors in $\mathcal{U}$ such that the array is in echelon form, since the first (leftmost) entry for $u(i,j,n-1,n)$ is at $\{i,j\}$. The ordering is as follows: $u(1,2,n-1,n), \ldots, u(1,n-2,n-1,n), u(2,3,n-1,n), \ldots, u(n-3,n-2,n-1,n)$ followed by $u(1,n-1,n,2), u(2,n-1,n,3), \ldots, u(n-3,n-1,n,n-2)$. Since $|\mathcal{U}| = (n-3)+(n-2)+\ldots+1+(n-3) = \binom{n}{2} - n = \dim(C_n^{\perp})$, we have the result. ■

Proposition 3 *For $n \geq 3$, $\mathrm{Aut}(\mathcal{G}_n) = S_n$; for $n \geq 5$, $\mathrm{Aut}(C_n) = S_n$.*

Proof: From Whitney's theorem [19] it follows that $\mathrm{Aut}(T_n) = \mathrm{Aut}(K_n) = S_n$ and thus $S_n \subseteq \mathrm{Aut}(\mathcal{G}_n)$. For the reverse inclusion, suppose that $\sigma \in \mathrm{Aut}(\mathcal{G}_n)$. To show that $\sigma \in \mathrm{Aut}(T_n)$, suppose P and Q are adjacent in T_n. Then $P = \{a,b\}$ and $Q = \{a,c\}$, so $P, Q \in \overline{a}$. Thus $P\sigma, Q\sigma \in \overline{x}$ for some $x \in \Omega$, and so $P\sigma$ and $Q\sigma$ are adjacent in T_n and hence $\sigma \in \mathrm{Aut}(T_n)$.

For $n \geq 6$, by Proposition 1, the words of weight $n-1$ are the scalar multiples of the blocks of $\mathcal{G}_n$. Since weight classes are preserved by any $\sigma \in \mathrm{Aut}(C_n)$, we see that $\sigma \in \mathrm{Aut}(\mathcal{G}_n) = S_n$, and thus $\mathrm{Aut}(C_n) = S_n$ for $n \geq 6$. For $n = 5$ there are other vectors of weight-4, but Magma [2, 5] tells us that the group is S_5. ■

Note: For $n = 4$, $\mathrm{Aut}(C_4) \neq S_4$, by Magma.

Proposition 4 *If $n \geq 5$, $C_n = C_p(\mathcal{G}_n)$ and p is any odd prime, then*

$$\mathcal{I}_n = \{\{1,n\},\ldots,\{n-1,n\},\{1,2\}\}$$

is an information set for C_n and

$$S = \{(n,i)(1,j) \mid 1 \leq i \leq n, 1 \leq j \leq n-1\},$$

where $(i,j) \in S_n$ is a transposition and (k,k) denotes the identity ι of S_n, is a PD-set of $n(n-1)$ elements for C_n using $\mathcal{I}_n$.

Proof: That $\mathcal{I}_n$ is an information set follows by looking at the matrix M_n and using the last $n-1$ coordinate positions, along with the first position. Let $\mathcal{C}$ be the corresponding check set.

C_n corrects $t = \lfloor \frac{n-2}{2} \rfloor$ errors. Let $\mathcal{T}$ be a set of $s \leq t$ points. If $\mathcal{T} \subseteq \mathcal{C}$, then the identity map ι can be used.

There are two cases for $\mathcal{T}$:

Case (i):

$$\mathcal{T} = \{\{a_1,n\},\ldots,\{a_r,n\}\} \cup \{\{b_1,c_1\},\ldots,\{b_m,c_m\}\},$$

where $r+m \leq t$, $r \geq 1$, $a_i, b_i, c_i \neq n$, $\{b_i,c_i\} \in \mathcal{C}$ for $1 \leq i \leq m$.

Let $T = \{a_1,\ldots,a_r\} \cup \{b_1,\ldots,b_m\} \cup \{c_1,\ldots,c_m\}$. Then

$$|T| \leq r + 2m < 2r + 2m \leq n-2,$$

so $|T| \leq n-3$ and there are at least three members of Ω not in T, one of which is n. Let $d, e \notin T \cup \{n\}$. Then (d,n) moves $\{a_i,n\}$ to $\{a_i,d\} \in \mathcal{C}$ if $d \neq 1,2$, and fixes the $\{b_i,c_i\}$. If $d,e = 1,2$ then $1,2 \notin T$, so $(1,n)$ moves $\{a_i,n\}$ to $\{a_i,1\} \in \mathcal{C}$ since $a_i \neq 2$.

Case (ii):

$$\mathcal{T} = \{\{a_1,n\},\ldots,\{a_{r-1},n\},\{1,2\}\} \cup \{\{b_1,c_1\},\ldots,\{b_m,c_m\}\},$$

where $r+m \leq t$, $r \geq 1$, $a_i, b_i, c_i \neq n$, $\{b_i,c_i\} \in \mathcal{C}$ for $1 \leq i \leq m$.

Let $T = \{a_1,\ldots,a_{r-1}\} \cup \{1,2\} \cup \{b_1,\ldots,b_m\} \cup \{c_1,\ldots,c_m\}$. Then

$$|T| \leq r + 1 + 2m \leq 2r + 2m \leq n-2,$$

so there exists $d \neq 1,2,n$ such that $d \notin T$. Then $(d,n)(d,1) = (d,n,1)$ maps $\{1,2\}$ to $\{d,2\}$, $\{1,c_i\}$ to $\{d,c_i\}$ and $\{a_i,n\}$ to $\{a_i,1\}$ which is in $\mathcal{C}$ unless $a_i = 2$ for some i. If $a_i = 2$ for some i, then

$|T| \leq r + 2m < n-2$ and so there is $e \neq 1,2,d,n$, such that $e \notin T$. Then $(n,d)(1,e)$ moves $\{1,2\}$ to $\{2,e\}$, $\{a_i,n\}$ to $\{a_i,d\}$ or $\{e,d\}$ if $a_i = 1$, and $\{1,c_i\}$ to $\{e,c_i\}$.

This completes the proof for all cases, so we have a PD-set. It is clear that all the elements of S as defined are distinct, and hence it has size $n(n-1)$. ■

Recall that the code $E_n = \langle\, v^{\overline{x}} - \, v^{\overline{y}} \mid x,y \in \Omega\rangle$ is defined in Equation (4).

Proposition 5 *For $n \geq 3$, p an odd prime, E_n has codimension 1 in C_n and $E_n = \mathrm{Hull}(\mathcal{G}_n)$ if and only if $n \equiv 2 \pmod{p}$.*

For $n \geq 8$ the minimum weight of E_n is $2n-4$. For $n = 7$ the minimum weight of E_n is at least $2n-5$. For $n \geq 9$ the minimum words of E_n are the scalar multiples of $\, v^{\overline{x}} - \, v^{\overline{y}}$ for $x,y \in \Omega$.

Proof: The $\, v^{\overline{x}}$ are linearly independent, so clearly $[C_n : E_n] = 1$. Now $(\, v^{\overline{x}} - \, v^{\overline{y}}, \, v^{\overline{z}}) = 0$ if x,y,z are distinct, $n-2$ if $x = z \neq y$. This proves the first part of the statement.

We consider the possibility of words of C_n of weight s in the range $n \leq s \leq 2n-5$, and show that this cannot happen if $n \geq 8$.

Let $w \in C_n$, $w = \sum_{i=1}^{n} \alpha_i \, v^{\overline{i}}$. Then $w(\{i,j\}) = \alpha_i + \alpha_j$. If exactly r of the α_i are non-zero, then $\mathrm{wt}(w) \geq r(n-r)$. If we write $f(r) = r(n-r)$ then note that $f(n-r) = f(r)$ and $f(r)$ has a maximum value at $r = n/2$. So if $\mathrm{wt}(w) = s$ where $n \leq s \leq 2n-5$, then $r = n-1$ or $r = n$. Let $\mathcal{S} = \mathrm{Supp}(w)$, and $s = |\mathcal{S}|$.

Suppose that $r = n-1$ and that $\alpha_n = 0$, $\alpha_i \neq 0$ for $1 \leq i \leq n-1$. Then $w(\{i,n\}) = \alpha_i + 0 \neq 0$ for $1 \leq i \leq n-1$, so $\, \overline{n} \subseteq \mathcal{S}$. Since $s \geq n$, $\mathcal{S} \neq \, \overline{n}$. For any three distinct i,j,k in $\{1,\ldots,n-1\}$, we cannot have $\alpha_i + \alpha_j = \alpha_i + \alpha_k = \alpha_j + \alpha_k = 0$, so every triple of elements in $\{1,\ldots,n-1\}$ has at least one of the three 2-subsets as a point in $\mathcal{S}$. Any point $\{i,j\}$, where $i,j \in \{1,\ldots,n-1\}$, is in $n-3$ triples on these points. There are $\binom{n-1}{3}$ such triples, so we need at least $\frac{(n-1)(n-2)}{6}$ points to **cover** all these triples, i.e. to ensure that every such triple has at least one 2-subset in $\mathcal{S}$. Thus

$$s \geq n-1 + \frac{(n-1)(n-2)}{6} = \frac{(n-1)(n+4)}{6} > 2n-5 \tag{15}$$

for all n, so this case is ruled out.

Suppose $r = n$, i.e. $\alpha_i \neq 0$ for $1 \leq i \leq n$. Arguing as in the previous case we have, since every pair is now in $n-2$ triples,

$$s \geq \frac{n(n-1)}{6} > 2n-5 \tag{16}$$

for $n \geq 11$, leaving $n = 7,8,9,10$ to eliminate.

We first consider generally how best to pick the points in $\mathcal{S}$ so as to get the smallest set to cover all the triples. Notice that two points $\{a,b\}$ and $\{c,d\}$ will not cover any common triples if a,b,c,d are all distinct, while $\{a,b\}$ and $\{a,c\}$ will both cover the triple $\{a,b,c\}$. Thus we attempt at first to choose as many non-intersecting points (as 2-sets), i.e. we take the $\lfloor \frac{n}{2} \rfloor$ points $\{i,i+1\}$ for $1 \leq i \leq n$ for n even, and $1 \leq i \leq n-1$ for n odd, and then add more points to cover the remaining triples. Note also that every member i of Ω must occur in some point in $\mathcal{S}$, since otherwise to cover all the triples containing i we would need $\binom{n-1}{2} > 2n-5$ points since each triple containing i would be covered by only one point of $\mathcal{S}$.

First take $n = 2m$ even and let $\mathcal{S}^* = \{\{1,2\},\ldots,\{n-1,n\}\}$. This covers $\frac{n(n-2)}{2}$ triples. A further point $\{a,b\}$ must be such that $\{a,c\},\{b,d\} \in \mathcal{S}^*$. Thus the triples $\{a,c,b\}$ and $\{b,d,a\}$ have already been counted, so any further point will cover at most $n-4$ new triples. So we need k of these points, where

$$k \geq \frac{1}{n-4}\left(\binom{n}{3} - \frac{n(n-2)}{2}\right).$$

Thus

$$s = \frac{n}{2} + k \geq \frac{n(n+1)}{6} > 2n-5$$

for $n \geq 8$. But for $n = 8, 10$ we still need to check if a choice of points not involving the largest possible coverage of triples might be made with fewer points. We will consider this after we deal with the case of n odd.

Suppose $n = 2m+1$. Choose $\mathcal{S}^* = \{\{1,2\},\ldots,\{n-2,n-1\}\}$, covering $\frac{(n-1)(n-2)}{2}$ triples. The points $\{i,n\}$ and $\{2,n\}$ will cover a further $n-3$ triples each, but further points will cover at most $n-4$ triples. We need k of these where

$$k \geq \frac{1}{n-4}\left(\binom{n}{3} - \frac{(n-1)(n-2)}{2} - 2(n-3)\right) = \frac{n^3-6n^2-n+30}{6(n-4)}.$$

Thus

$$s = \frac{n-1}{2} + 2 + k \geq \frac{(n+3)}{2} + \frac{n^3-6n^2-n+30}{6(n-4)} > 2n-5,$$

i.e. for $(n-7)(n^2-8n+18) > 0$, on simplifying, so for $n \geq 9$. For $n = 7$ the word $\sum_{i=1}^{3} v^{\bar{i}} - \sum_{i=4}^{7} v^{\bar{i}}$ has weight 9; it is in C_n but not in E_n.

We still need to consider the possibility of getting a smaller word by a different choice of points, i.e. by not taking the maximal number of mutually disjoint 2-sets.

For $n = 7$, suppose $\mathcal{S}$ has at most two points from disjoint 2-sets, say $\{1,2\},\{3,4\}$. To satisfy this condition, every other point in $\mathcal{S}$ must contain at least one of $1,2,3,4$. Thus the triple $\{5,6,7\}$ cannot be covered, so this possibility is ruled out. This argument shows that the choice we have made above in the odd case is the only possibility, and the argument applies equally well to $n = 9$. Thus for $n = 9$ the minimum weight of E_n is $14 = 2n-4$.

For $n = 8$, suppose $\mathcal{S}$ has at most three points, say $\{1,2\},\{3,4\},\{5,6\}$, from disjoint 2-sets. These will cover 18 triples. We need points containing 7 and 8, but not both together, and we show that we can find at most four that each cover a new set of five triples, and thus 20 amongst them. We can take $\{1,7\}$ as the next point, covering five new triples, and then not choose $\{1,8\}$ (covering only four new triples), nor $\{2,8\}$ (would give four disjoint 2-sets), and so $\{3,8\}$ for our next point, covering five new triples. The points $\{2,7\},\{4,8\}$ will then cover a further five triples each. So far $\mathcal{S} = \{\{1,2\},\{3,4\},\{5,6\},\{1,7\},\{2,7\},\{3,8\},\{4,8\}\}$. All members of Ω are now covered, but only 38 of the 56 triples. A further point $\{a,b\} \notin \mathcal{S}$ must have $\{a,a'\}$ and $\{b,b'\}$ in $\mathcal{S}$. The two triples $\{a,b,a'\}$ and $\{a,b,b'\}$ will be distinct, by our choice of $\mathcal{S}$ so far (since if $a' = b'$ then $\{a,b\}$ is already in $\mathcal{S}$), and will already be covered. Thus all remaining extra points will cover at most four triples each. Thus we will need k of them, where $4k \geq 56-18-20 = 18$, i.e. $k \geq 5$, and $s \geq 3+4+5 = 12$. The cases of at most two or less disjoint 2-sets can be ruled out as in the case for $n = 7$ or 9 above. So the minimum weight of E_n for $n = 8$ is $12 = 2n-4$.

For $n = 10$, $n-2 = 8$, so if there are at most four disjoint 2-sets, then we can get at most seven new triples from further points, so we need a further k points, where $7k \geq 120-32$, i.e. $k \geq 13$, so $s \geq 17 > 2n-5 = 15$. The cases of at most three or less disjoint 2-sets can be ruled out as in the case for $n = 7$ or 9 above. So the minimum weight of E_n for $n = 10$ is $16 = 2n-4$.

We now show that words of weight $2(n-2)$ in C_n must be scalar multiples of $v^{\overline{x}} - v^{\overline{y}}$, $x, y \in \Omega$ if $n \geq 9$. As before, let $w \in C_n$, $w = \sum_{i=1}^{n} \alpha_i \, v^{\overline{i}}$, and $\mathrm{wt}(w) = 2(n-2)$. If exactly r of the α_i are non-zero, then $\mathrm{wt}(w) \geq r(n-r)$. If $r = 2$ then clearly $w = \alpha(v^{\overline{x}} - v^{\overline{y}})$. Otherwise, since $f(n-2) = f(2)$, we could have $r = n-2, n-1, n$; we will show that none of these possibilities can give a word of weight $2(n-2)$. Our arguments will follow those used above to establish the minimum weight.

Suppose $r = n-2$, and that $\alpha_{n-1} = \alpha_n = 0$. Then $w(\{i,n\}) = w(\{i,n-1\}) = \alpha_i \neq 0$ for $1 \leq i \leq n-2$, and $\mathrm{Supp}(w) = \overline{n} \cup \overline{n-1} \setminus \{\{n-1,n\}\}$. Then $w - \alpha_1(v^{\overline{n}} - v^{\overline{n-1}})$ will have weight at most $2n-5$ and can only be a scalar multiple of some $v^{\overline{i}}$. This gives a contradiction since the $v^{\overline{j}}$ are linearly independent. Thus this cannot happen.

If $r = n-1$, $\alpha_n = 0$, then the earlier argument yields that $\overline{n} \subseteq \mathrm{Supp}(w)$. Thus $w - \alpha_1 \, v^{\overline{n}}$ will have weight less than $2n-4$, and thus must be $\beta \, v^{\overline{i}}$ for some $i \neq n$. Thus $w = \alpha_1 \, v^{\overline{n}} + \beta \, v^{\overline{i}}$, which is not possible, as before.

If $r = n$, then Equation (16) will give $6(2n-4) \geq n(n-1)$ which is impossible for $n \geq 11$. Again we are left with $n = 9, 10$. The arguments we used before go through similarly to rule out this eventuality. Thus a word of weight $2(n-2)$ can only be obtained from scalar multiples of the vectors $v^{\overline{x}} - v^{\overline{y}}$.

This completes the proof. ■

Note: For $n = 6$ the minimum weight of E_n is $6 = 2n-6$. This is found by observing that for n even, $n = 2m$, the word $w = \sum_{i=1}^{m} v^{\overline{i}} - \sum_{i=m+1}^{n} v^{\overline{i}} \in E_n$ and has weight $m(m-1)$. For $n = 6$ this gives words of weight 6; for $n = 8$ it gives words of weight 12 that are not scalar multiples of vectors $v^{\overline{x}} - v^{\overline{y}}$, $x, y \in \Omega$. More generally, $\sum_{i=1}^{r} v^{\overline{i}} - \sum_{i=r+1}^{n} v^{\overline{i}}$ for all $r \leq n$, has weight $\binom{r}{2} + \binom{n-r}{2}$ which is outside our range for $n > 8$. However, for $n = 7$ it gives words of weight 9 (taking $r = 3$) in C_n (but not in E_n), in the range $7 \leq s \leq 9 = 2n-5$. Here $2n-6 = 8$, which we have eliminated. However, these words generally are in E_n only if n is even.

Proposition 6 *For $n \geq 4$, p an odd prime,*

$$\mathcal{I}_n^* = \{\{1,n\},\{2,n\},\ldots,\{n-2,n\},\{1,2\}\}$$

is an information set for E_n and for $n \geq 7$,

$$S^* = \{(n-1,i)(n,j)(1,k) \mid 1 \leq i \leq n-1, 1 \leq j \leq n, 3 \leq k \leq n-1\},$$

is a PD-set of size $n(n^2-5n+7)$ for E_n to correct $n-3$ errors, using $\mathcal{I}_n^*$.

Proof: To show that $\mathcal{I}_n^*$ is an information set, consider the matrix M_n, and bring the last $n-1$ columns to the front, as in Proposition 1. Use the words $v^{\overline{1}} - v^{\overline{i}}$, for $2 \leq i \leq n$ to get a generator matrix for E_n. Now it is easy to see that the first $n-1$ columns will give an information set for E_n if $n \not\equiv 2 \pmod{p}$, but replacing the column headed by $\{n-1,n\}$ by that of $\{1,2\}$ will give an information set for all n.

Let $\mathcal{C}$ denote the check set and write $\mathcal{I} = \mathcal{I}_n^*$. Let $\mathcal{T}$ be a set of $t \leq n-3$ points of $\mathcal{P}_n$. If $\mathcal{T} \subseteq \mathcal{C}$ then we can use ι. Let $\mathcal{T} \cap \mathcal{I} = \mathcal{I}_T$ and $\mathcal{T} \cap \mathcal{C} = \mathcal{C}_T$. There are two cases for $\mathcal{T}$:
Case (i):

$$\mathcal{T} = \{\{a_1,n\},\ldots,\{a_r,n\}\} \cup \{\{b_1,c_1\},\ldots,\{b_m,c_m\}\}$$

Case (ii):

$$\mathcal{T} = \{\{a_1, n\}, \dots, \{a_{r-1}, n\}, \{1, 2\}\} \cup \{\{b_1, c_1\}, \dots, \{b_m, c_m\}\},$$

where $r + m = t$, $r \geq 1$, and $\{a_1, \dots, a_r\} \subset \Omega \setminus \{n-1, n\}$.

In Case (i), let $T = \{a_1, \dots, a_r\} \cup \{b_1, \dots, b_m\} \cup \{c_1, \dots, c_m\}$, where $r \geq 1$. If there exists $i \in T$, $i \neq 1, 2, n$, then $(i, n) : \{a_j, n\} \mapsto \{a_j, i\} \in \mathcal{C}$, fixes $\{b_j, c_j\}$ except possibly for $\{n-1, n\} \mapsto \{n-1, i\} \in \mathcal{C}$, since $i \neq n - 1$ in this eventuality.

In Case (ii), let $T = \{a_1, \dots, a_{r-1}\} \cup \{1, 2\} \cup \{b_1, \dots, b_m\} \cup \{c_1, \dots, c_m\}$, where $r \geq 1$. If there exists $i \in T$, $i \neq 1, 2, n$, then there is $j \neq 1, 2, n$ such that $\{2, j\} \notin \mathcal{T}(i, n)$, since $|\{\{2, 3\}, \dots, \{2, n-1\}\}| = n - 3$, but $|\mathcal{T}(i, n) \cap \mathcal{C}| \leq n - 4$ (since $\{1, 2\} \in \mathcal{T}(i, n)$), so the map $\tau = (i, n)(1, j)$ will work. If $r = 1$ then $(1, j)$ will suffice.

Now consider the general Case (i) or (ii) in which every element of Ω occurs in T where T is as given above, respectively for (i) or (ii). We show that there is some $i \neq n, n-1$ such that i occurs only once in the set $\mathcal{C}_T = \{\{b_1, c_1\}, \dots, \{b_m, c_m\}\}$. For any $i \in \Omega$ let n_i be the number of times i occurs in this set. Then $2m = \sum_{i=1}^{n} n_i$, $n_n \leq 1$, and $n_i = 0$ for at most r values of i in Case (i), or at most $r - 1$ values of i in Case (ii). Suppose $n_i \geq 2$ for all the i that occur in $\mathcal{C}_T$, excluding $i = n, n-1$. Then $2m = \sum n_i \geq 2(n - r - 2)$ in either case, i.e. $m + r \geq n - 2$, which is a contradiction.

Thus let i occur only once in $\mathcal{C}_T$, as $\{i, j\}$. Then the map $(n-1, j)(n, i)$ followed by $(1, k)$ where $\{2, k\} \notin \mathcal{T}(n-1, j)(n, i)$ if necessary, will map $\mathcal{T}$ into $\mathcal{C}$.

Finally the size of S^* is $n(n-1)(n-3) - n(n-4) = n(n^2 - 5n + 7)$, since there are $n(n-4)$ repeats amongst the shown elements, as can easily be verified. ■

5 The codes $\overline{C}_n, \overline{\overline{C}}_n, \widetilde{C}_n, \widetilde{\widetilde{C}}_n$

We show now that none of the p-ary codes, for p odd, from the triangular graph nor its complementary graph, nor from the reflexive graphs, give any interesting new codes beyond the codes C_n and E_n, and their duals, that we have already examined. In fact, even in the binary case the codes in Result 1 are C_n for n odd and E_n for n even. Thus our results, along with those from Result 1, give PD-sets for these codes over all primes.

We use the notation established in Section 3.

Lemma 2 *For all $n \geq 4$, all odd primes p, the weight-4 vectors $u(a, b, c, d)$ of Equation (14) are in each of $\overline{C}_n, \overline{\overline{C}}_n, \widetilde{C}_n, \widetilde{\widetilde{C}}_n$.*

Proof: It can be verified easily that, if we write $u = u(a, b, c, d)$, then

$$v^{\overline{\{a,b\}}} + v^{\overline{\{c,d\}}} - v^{\overline{\{a,c\}}} - v^{\overline{\{b,d\}}} = -2u.$$

It then follows from Equations (7) and (13) that

$$\begin{aligned}
v^{\overline{\overline{\{a,b\}}}} + v^{\overline{\overline{\{c,d\}}}} - v^{\overline{\overline{\{a,c\}}}} - v^{\overline{\overline{\{b,d\}}}} &= -u \\
v^{\widetilde{\{a,b\}}} + v^{\widetilde{\{c,d\}}} - v^{\widetilde{\{a,c\}}} - v^{\widetilde{\{b,d\}}} &= u \\
v^{\widetilde{\widetilde{\{a,b\}}}} + v^{\widetilde{\widetilde{\{c,d\}}}} - v^{\widetilde{\widetilde{\{a,c\}}}} - v^{\widetilde{\widetilde{\{b,d\}}}} &= 2u,
\end{aligned}$$

which gives the result. ■

Note that in the binary case $\overline{\overline{C}}_n$ and $\widetilde{C}_n$ contain the weight-4 vector u.

Proposition 7 *For $n \geq 4$, all odd primes p,*

1. *if $n \equiv 4 \pmod{p}$ then $\overline{C}_n = E_n^{\perp}$; if $n \not\equiv 4 \pmod{p}$ then $\overline{C}_n = \mathbb{F}_p^{\binom{n}{2}}$ if $n \not\equiv 2 \pmod{p}$, and $\overline{C}_n = \langle \boldsymbol{\jmath} \rangle^{\perp}$ for $n \equiv 2 \pmod{p}$;*

2. *if $n \equiv 3 \pmod{p}$ then $\overline{\overline{C}}_n = E_n^{\perp}$; if $n \not\equiv 3 \pmod{p}$ then $\overline{\overline{C}}_n = \mathbb{F}_p^{\binom{n}{2}}$ if $2n \not\equiv 3 \pmod{p}$, and $\overline{\overline{C}}_n = \langle \boldsymbol{\jmath} \rangle^{\perp}$ for $2n \equiv 3 \pmod{p}$;*

3. *if $n \equiv 3 \pmod{p}$ then $\widetilde{C_n} = C_n^{\perp}$; if $n \equiv 2 \pmod{p}$ then $\widetilde{C_n} = \langle \boldsymbol{\jmath} \rangle^{\perp}$; if $n \not\equiv 2, 3 \pmod{p}$ then $\widetilde{C_n} = \mathbb{F}_p^{\binom{n}{2}}$;*

4. *if $n \equiv 4 \pmod{p}$ then $\widetilde{\widetilde{C_n}} = E_n^{\perp}$; if $n \not\equiv 4 \pmod{p}$ then $\widetilde{\widetilde{C_n}} = \mathbb{F}_p^{\binom{n}{2}}$ if $n^2 - 5n + 8 \not\equiv 0 \pmod{p}$, and $\widetilde{\widetilde{C_n}} = \langle \boldsymbol{\jmath} \rangle^{\perp}$ for $n^2 - 5n + 8 \equiv 0 \pmod{p}$.*

Proof: Writing $\Omega = \{1, 2, \ldots, n\}$, let $u(1,2,3) = \sum_{i=4}^{n} u(1,2,3,i) = \sum_{i=4}^{n}(v^{\{1,2\}} + v^{\{3,i\}} - v^{\{1,3\}} - v^{\{2,i\}})$. Then it follows that

$$u(1,2,3) = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) - \sum_{i \neq 3} v^{\{2,i\}} + \sum_{i \neq 2} v^{\{3,i\}},$$

and $u(1,2,3) \in \overline{C}_n, \overline{\overline{C}}_n, \widetilde{C_n}, \widetilde{\widetilde{C_n}}$ by Lemma 2. Now we consider the four classes of codes, the proofs being similar.

1. For $\overline{C}_n$:

   $$v^{\overline{\{1,3\}}} - v^{\overline{\{1,2\}}} + v^{\overline{\{2,3\}}} = 2(v^{\{1,2\}} + \sum_{i=4}^{n} v^{\{3,i\}}) = \bar{v}, \tag{17}$$

   is in $\overline{C}_n$.

   Now $w = u(1,2,3) + v^{\overline{\{2,3\}}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i \neq 2}^{n} v^{\{3,i\}} \in \overline{C}_n$, and so $w - \bar{v} = (n-4)(v^{\{1,2\}} - v^{\{1,3\}}) \in \overline{C}_n$. If $n \not\equiv 4 \pmod{p}$ then $v^{\{1,2\}} - v^{\{1,3\}} \in \overline{C}_n$, and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^{\perp} \subseteq \overline{C}_n$. But $\boldsymbol{\jmath} \in \overline{C}_n^{\perp}$ only if $n \equiv 2 \pmod{p}$, so we have the stated result for $n \not\equiv 4 \pmod{p}$.

   If $n \equiv 4 \pmod{p}$, then since $(v^{\overline{x}}, v^{\overline{\{y,z\}}}) = 2$ if $x \neq y, z$ and $n-2$ if $x = y$ or z, it follows that $\overline{C}_n \subseteq E_n^{\perp}$. Now from Proposition 2, the weight-4 vectors span $C_n^{\perp}$, so $C_n^{\perp} \subseteq \overline{C}_n$. Clearly we cannot have equality, and since $[E_n^{\perp} : C_n^{\perp}] = 1$, we have $\overline{C}_n = E_n^{\perp}$.

2. For $\overline{\overline{C}}_n$:

   $$\begin{aligned} v^{\overline{\overline{\{1,3\}}}} - v^{\overline{\overline{\{1,2\}}}} + v^{\overline{\overline{\{2,3\}}}} &= 2(v^{\{1,2\}} + \sum_{i=4}^{n} v^{\{3,i\}}) + v^{\{1,3\}} - v^{\{1,2\}} + v^{\{2,3\}} \\ &= v^{\{1,2\}} - v^{\{1,3\}} - v^{\{2,3\}} + 2\sum_{i \neq 3}^{n} v^{\{3,i\}} = \overline{\overline{v}}, \end{aligned}$$

   using Equation (17), is in $\overline{\overline{C}}_n$.

Now $v = u(1,2,3) + v^{\overline{\overline{\{2,3\}}}} = u(1,2,3) + v^{\overline{\{2,3\}}} + v^{\{2,3\}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i\neq 2}^{n} v^{\{3,i\}} + v^{\overline{\{2,3\}}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i\neq 3}^{n} v^{\{3,i\}} - v^{\overline{\{2,3\}}} \in \overline{\overline{C}}_n$, so $v - \overline{\overline{v}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i\neq 3}^{n} v^{\{3,i\}} - v^{\overline{\{2,3\}}} - (v^{\{1,2\}} - v^{\{1,3\}} - v^{\{2,3\}} + 2\sum_{i\neq 3}^{n} v^{\{3,i\}}) = (n-3)(v^{\{1,2\}} - v^{\{1,3\}}) \in \overline{\overline{C}}_n$. If $n \not\equiv 3 \pmod{p}$ then $v^{\{1,2\}} - v^{\{1,3\}} \in \overline{\overline{C}}_n$, and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^\perp \subseteq \overline{\overline{C}}_n$. But $\boldsymbol{\jmath} \in \overline{\overline{C}}_n^{\perp}$ only if $2n \equiv 3 \pmod{p}$, so we have the stated result for $n \not\equiv 3 \pmod{p}$.

If $n \equiv 3 \pmod{p}$, then since $(v^{\overline{x}}, v^{\overline{\{y,z\}}}) = 2$ if $x \neq y, z$ and $n-1$ if $x = y$ or z, it follows that $\overline{\overline{C}}_n \subseteq E_n^\perp$. Now from Proposition 2, the weight-4 vectors span $C_n^\perp$, so $C_n^\perp \subseteq \overline{\overline{C}}_n$. Clearly we cannot have equality, and since $[E_n^\perp : C_n^\perp] = 1$, we have $\overline{\overline{C}}_n = E_n^\perp$.

3. For $\widetilde{C}_n$:

$$\begin{aligned} v^{\widetilde{\{1,3\}}} - v^{\widetilde{\{1,2\}}} + v^{\widetilde{\{2,3\}}} &= (\boldsymbol{\jmath} - v^{\overline{\overline{\{1,3\}}}}) - (\boldsymbol{\jmath} - v^{\overline{\overline{\{1,2\}}}}) + (\boldsymbol{\jmath} - v^{\overline{\overline{\{1,3\}}}}) \\ &= \boldsymbol{\jmath} - (v^{\{1,2\}} - v^{\{1,3\}} - v^{\{2,3\}} + 2\sum_{i\neq 3}^{n} v^{\{3,i\}}) = \tilde{v}, \end{aligned}$$

from the equation for $\overline{\overline{v}}$ in the previous case, is in $\widetilde{C}_n$.

Now writing $v = u(1,2,3) - v^{\widetilde{\{2,3\}}} = u(1,2,3) - \boldsymbol{\jmath} + v^{\overline{\{2,3\}}} + v^{\{2,3\}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i\neq 2}^{n} v^{\{3,i\}} - \boldsymbol{\jmath} + v^{\{2,3\}}$, then $v + \tilde{v} = (n-3)(v^{\{1,2\}} - v^{\{1,3\}}) \in \widetilde{C}_n$. If $n \not\equiv 3 \pmod{p}$ then $v^{\{1,2\}} - v^{\{1,3\}} \in \widetilde{C}_n$, and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^\perp \subseteq \widetilde{C}_n$. But $\boldsymbol{\jmath} \in \widetilde{C}_n^{\perp}$ only if $n \equiv 2 \pmod{p}$, so we have the stated result for $n \not\equiv 3 \pmod{p}$.

If $n \equiv 3 \pmod{p}$, then since $(v^{\overline{x}}, v^{\overline{\{y,z\}}}) = n-3$ if $x \neq y, z$ and 0 if $x = y$ or z, it follows that $\widetilde{C}_n \subseteq C_n^\perp$. Now from Proposition 2, the weight-4 vectors span $C_n^\perp$, so $C_n^\perp \subseteq \widetilde{C}_n$, and thus we have equality.

4. For $\widetilde{\widetilde{C}}_n$,

$$\begin{aligned} v^{\widetilde{\widetilde{\{1,3\}}}} - v^{\widetilde{\widetilde{\{1,2\}}}} + v^{\widetilde{\widetilde{\{2,3\}}}} &= \tilde{v} + v^{\{1,3\}} - v^{\{1,2\}} + v^{\{2,3\}} \\ &= \boldsymbol{\jmath} - 2(v^{\{1,2\}} - v^{\{1,3\}} - v^{\{2,3\}}) - 2\sum_{i\neq 3}^{n} v^{\{3,i\}} = \tilde{\tilde{v}}, \end{aligned}$$

from the last case, so $\tilde{\tilde{v}} \in \widetilde{\widetilde{C}}_n$.

Now writing $v = u(1,2,3) - v^{\widetilde{\widetilde{\{2,3\}}}} = (n-2)(v^{\{1,2\}} - v^{\{1,3\}}) + 2\sum_{i\neq 2}^{n} v^{\{3,i\}} - \boldsymbol{\jmath}$, then $v + \tilde{\tilde{v}} = (n-4)(v^{\{1,2\}} - v^{\{1,3\}}) \in \widetilde{\widetilde{C}}_n$. If $n \not\equiv 4 \pmod{p}$ then $v^{\{1,2\}} - v^{\{1,3\}} \in \widetilde{\widetilde{C}}_n$, and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^\perp \subseteq \widetilde{\widetilde{C}}_n$. But $\boldsymbol{\jmath} \in \widetilde{\widetilde{C}}_n^{\perp}$ only if $n^2 - 5n + 8 \equiv 0 \pmod{p}$, so we have the stated result for $n \not\equiv 4 \pmod{p}$.

If $n \equiv 4 \pmod{p}$, then since $(v^{\overline{x}}, v^{\overline{\{y,z\}}}) = n-3$ if $x \neq y, z$ and 1 if $x = y$ or z, it follows that $\widetilde{\widetilde{C}}_n \subseteq E_n^\perp$. Now from Proposition 2, the weight-4 vectors span $C_n^\perp$, so $C_n^\perp \subseteq \widetilde{\widetilde{C}}_n$. Clearly we cannot have equality, and since $[E_n^\perp : C_n^\perp] = 1$, we have $\widetilde{\widetilde{C}}_n = E_n^\perp$.

This completes all the cases. ■

Acknowledgement

J. D. Key thanks the School of Mathematical Sciences at the University of KwaZula-Natal for their hospitality in November 2008.

References

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

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

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

[4] A. E. Brouwer and J.H. van Lint. Strongly regular graphs and partial geometries. In D.M. Jackson and S.A. Vanstone, editors, *Enumeration and Design*, pages 85–122. Toronto: Academic Press, 1984. Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982.

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

[6] Washiela Fish. *Codes from uniform subset graphs and cyclic products.* PhD thesis, University of the Western Cape, 2007.

[7] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[8] Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel. Binary codes of strongly regular graphs. *Des. Codes Cryptogr.*, 17:187–209, 1999.

[9] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[10] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding for codes from finite planes. *European J. Combin.*, 26:665–682, 2005.

[11] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25:113–123, 2004.

[12] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

[13] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

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

[15] René Peeters. On the p-ranks of the adjacency matrices of distance-regular graphs. *J. Algebraic Combin.*, 15:127–149, 2002.

[16] B. G. Rodrigues. *Codes of designs and graphs from finite simple groups.* PhD thesis, University of Natal, 2003.

[17] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[18] Vladimir D. Tonchev. *Combinatorial Configurations, Designs, Codes, Graphs.* Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 40. New York: Longman, 1988. Translated from the Bulgarian by Robert A. Melter.

[19] Hassler Whitney. Congruent graphs and the connectivity of graphs. *Amer. J. Math.*, 54:154–168, 1932.