Codes from lattice and related graphs, and permutation decoding

J. D. Key
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

June 30, 2010

Abstract

Codes of length n^2 and dimension $2n-1$ or $2n-2$ over the field $\mathbb{F}_p$, for any prime p, that can be obtained from designs associated with the complete bipartite graph $K_{n,n}$ and its line graph, the lattice graph, are examined. The parameters of the codes for all primes are obtained and PD-sets are found for full permutation decoding for all integers $n \geq 3$.

1 Introduction

Codes obtained from an adjacency matrix of the line graph of a graph are closely related to codes from an incidence matrix of the original graph, and are, in fact, subcodes of this in the binary case. The codes from the incidence matrix of a graph, in case the graph has some regularity, have been found, in many cases, to have rank either the number v of vertices, or $v-1$, in particular the latter in the binary case: see [6, 7, 13]. Furthermore, their minimum weight is often the valency of the graph, and the minimum words simply the scalar multiples of the rows of the matrix. Thus it makes sense to look at these codes in conjunction with the codes from the adjacency matrix of the line graph, and codes associated with this adjacency matrix. In addition, binary codes from some line graphs have been found to be good candidates for permutation decoding: see [6, 12, 16, 14, 15, 22].

In this paper we consider the lattice graph, where, for any n, the lattice graph is defined to be the line graph of the complete bipartite graph $K_{n,n}$. It is a strongly regular graph on $v = n^2$ vertices. The binary codes from the span of adjacency matrices of lattice graphs have been examined by various authors: see [3, 4, 9, 23], and with a view to permutation decoding in [16, 22]. We extend these results now to p-ary codes for all primes p; the p-rank of these and related graphs was examined in [20]. Taking the complete bipartite graph $K_{n,n}$ to have vertices from two disjoint sets $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$, the vertices of the lattice graph L_n are the n^2 pairs (a_i, b_j) with (a_i, b_j) and (a_k, b_m) adjacent if $i = k$ or $j = m$. If A_n denotes an adjacency matrix for L_n then $B_n = J - I - A_n$, where J is the all-one and I the identity $n^2 \times n^2$ matrix, will be an adjacency matrix for the the graph $\widetilde{L}_n$ on the same vertices with adjacency defined by (a_i, b_j) adjacent to (a_k, b_m) if $i \neq k, j \neq m$. We examine the neighbourhood designs and p-ary codes, for any 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 graph $K_{n,n}$, noting that $M_n^T M_n = A_n + 2I$. Thus the codes from the row span of M_n, 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 L_n^R and $\widetilde{L}_n^R$ obtained from L_n and $\widetilde{L}_n$, 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 $L_n, \tilde{L}_n, L_n^R, \tilde{L}_n^R$ are given as propositions and lemmas in the following sections. The notation is as explained in the paragraph above.

Theorem 1 *Let C_n be the p-ary code of an incidence matrix M_n for the complete bipartite graph $K_{n,n}$ where p is a prime and $n \geq 3$. The vertex set of $K_{n,n}$ is $A \cup B$, where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ and the edges are the pairs (a_i, b_j) where $a_i \in A$, $b_j \in B$. Then C_n is a $[n^2, 2n-1, n]_p$ code with information set*

$$\mathcal{I}_n = \{(a_i, b_n) \mid 1 \leq i \leq n\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n-1\}.$$

For $n \geq 3$, the minimum words are the scalar multiples of the rows r_i of M_n, and $\mathrm{Aut}(C_n) = S_n \wr S_2$, where $\mathrm{Aut}(C_n)$ denotes the automorphism group of C_n. The set

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

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

Let $E_n = \langle r_i - r_j \mid r_i, r_j \text{ rows of } M_n \rangle$. Then for $n \geq 3$, E_n is an $[n^2, 2n-2, 2n-2]_p$ code and the minimum words are the scalar multiples of the $r_i - r_j$. Further, $\mathcal{I}_n^* = \mathcal{I}_n \setminus \{(a_1, b_n)\}$ is an information set, and

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

a PD-set of size n^2 for E_n using $\mathcal{I}_n^*$.

The p-ary codes from $L_n, \widetilde{L}_n, L_n^R, \widetilde{L}_n^R$ are either $\mathbb{F}_p^{n^2}$, $\langle \jmath \rangle^\perp$, $C_n^\perp$, $E_n^\perp$, C_n or E_n.

We note that the binary code from the lattice graph is E_n: see Result 2 in Section 2.

The proof of the theorem follows from propositions and lemmas in the following sections. The full details about the codes from $L_n, \widetilde{L}_n, L_n^R, \widetilde{L}_n^R$ are in Proposition 8. Background definitions are given in Section 2, and notation for the graphs, designs and codes that we consider here is given in Section 3. Computations leading to these results were all done with Magma [5, 2].

2 Background and terminology

Notation for designs and codes is as in [1, Chapters 1,2]. 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** $C_F(\mathcal{D})$ **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 $v^{\mathcal{Q}}$, 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 $P \in \mathcal{P}$, $w(P)$ denotes the value of w at P. If $F = \mathbb{F}_p$ then the p**-rank** of the design, written $\mathrm{rank}_p(\mathcal{D})$, is the dimension of its code $C_F(\mathcal{D})$, which we usually write as $C_p(\mathcal{D})$.

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**, $\mathrm{wt}(v)$, of a vector v is the number of non-zero coordinate entries. 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. $C^\perp = \{v \in F^n | (v,c) = 0 \text{ for all } c \in C\}$. A code is **self-orthogonal** if $C \subseteq C^\perp$. A self-orthogonal binary code is **doubly − even** if all the codewords have weight divisible by 4. 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. We call two linear codes **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 first k coordinates in the standard form are the **information symbols** and the last $n-k$ coordinates are the **check symbols**.

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**. The **order** of $\Gamma = (V, E)$ is $|V|$. A graph is **regular** if all the vertices have the same valency. An **adjacency matrix** A of a graph of order $|V| = n$ 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. The **line graph** of a graph $\Gamma = (V, E)$ is the graph $L(\Gamma)$ with E as vertex set and where adjacency is defined so that e and f in E, as vertices, are adjacent in $L(\Gamma)$ if e and f as edges of Γ share a vertex in Γ. A **strongly regular graph** Γ of type (n, k, λ, μ) is a regular graph on $n = |V|$ vertices, with valency k which is such that any two adjacent vertices are together adjacent to λ vertices and any two non-adjacent vertices are together adjacent to μ vertices.

The **complete bipartite graph** $K_{n,n}$ on $2n$ vertices, $A \cup B$, where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$, with n^2 edges, has for line graph, the **lattice graph** L_n, which has vertex set the set of ordered pairs $\{(a_i, b_j) \mid 1 \leq i, j \leq n\}$, where two pairs are adjacent if and only if they have a common coordinate. L_n is a strongly regular graph of type $(n^2, 2(n-1), n-2, 2)$.

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 [18], involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [19, Chapter 16, p. 513] and Huffman [10, Section 8]. In [11] and [17] 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 [10] and requires that the generator matrix is in standard form. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [8] from a counting argument in [21], and quoted and proved in [10]:

Result 1 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$ code C, and $r = n-k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

PD-sets for binary codes from the lattice graphs were found in [16], in which the main result was as follows:

Result 2 *For $n \geq 5$, let C be the binary code from the row span of an adjacency matrix for the lattice graph of $K_{n,n}$ with vertices $A \times B$ where $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$. Then C is a $[n^2, 2(n-1), 2(n-1)]_2$ code and the set*

$$\mathcal{I} = \{(a_i, b_n) \mid 2 \leq i \leq n-1\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n\}$$

is an information set. The set

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

of permutations in $S_n \times S_n$ forms a PD-set of size n^2 for C for $\mathcal{I}$.

Note: Here, and in what follows, $t_{i,j}$ denotes the transposition $(i,j) \in S_n$, and $t_{k,k}$ denotes the identity element of S_n. This notation is used since we are using ordered pairs for the edges of $K_{n,n}$. The code C in the result is the code E_n of Theorem 1 for $p = 2$.

3 The graphs, designs and codes

In all the following sections, p will denote any prime. We set up our notation for the graphs, designs and codes that we will be examining.

For any $n \geq 2$, let $\mathcal{G}_n$ denote the incidence design of the complete bipartite graph $K_{n,n}$. Thus $\mathcal{G}_n$ is a 1-$(n^2, n, 2)$ design. The point set of $\mathcal{G}_n$ will be denoted by $\mathcal{P}_n = A \times B$, where $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$. This is the point set for all the classes of designs here. Writing $\Omega = \{1, \ldots, n\}$, we take for incidence matrix M_n where the first n rows are labelled by the vertices of $K_{n,n}$ in A, and the next n rows by B. The columns are labelled

$$(a_1, b_1), \ldots, (a_1, b_n), (a_2, b_1) \ldots (a_2, b_n), \ldots, (a_n, b_1), \ldots, (a_n, b_n). \tag{1}$$

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

$$\overline{a_i} = \{(a_i, b_j) \mid 1 \leq j \leq n\}, \tag{2}$$

and for $b_i \in B$ the block of $\mathcal{G}_n$ defined by the row b_i will be written as

$$\overline{b_i} = \{(a_j, b_i) \mid 1 \leq j \leq n\}. \tag{3}$$

The code of $\mathcal{G}_n$ over $\mathbb{F}_p$ will be denoted by C_n, assuming the prime p is clear from the context. Thus

$$C_n = \langle v^{\overline{x}} \mid x \in A \cup B \rangle, \tag{4}$$

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

$$E_n = \langle v^{\overline{x}} - v^{\overline{y}} \mid x, y \in A \cup B \rangle, \tag{5}$$

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

The lattice graph L_n is the line graph $L(K_{n,n})$. The rows of an adjacency matrix A_n for L_n give the blocks of the neighbourhood design $\overline{\mathcal{D}}_n$ of L_n. It is clear that $M_n^T M_n = A_n + 2I$. The blocks of $\overline{\mathcal{D}}_n$ are

$$\overline{(a_i, b_j)} = \{(a_i, b_k) \mid k \neq j\} \cup \{(a_k, b_j) \mid k \neq i\} \tag{6}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$. Thus $\overline{\mathcal{D}}_n$ is a symmetric 1-$(n^2, 2(n-1), 2(n-1))$ design for $n \geq 3$. We write

$$\overline{C}_n = \langle v^{\overline{(a_i,b_j)}} \mid (a_i, b_j) \in \mathcal{P}_n \rangle. \tag{7}$$

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

$$\overline{\overline{(a_i, b_j)}} = \overline{(a_i, b_j)} \cup \{(a_i, b_j)\} \tag{8}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\overline{\overline{C}}_n = \langle v^{\overline{\overline{(a_i,b_j)}}} \mid (a_i, b_j) \in \mathcal{P}_n \rangle. \tag{9}$$

The graph $\widetilde{L}_n$ is the complement of L_n and gives a symmetric 1-$(n^2, (n-1)^2, (n-1)^2)$ design $\widetilde{\mathcal{D}}_n$ with blocks

$$\widetilde{(a_i, b_j)} = \{(a_k, b_m) \mid k \neq i, m \neq j\} = \mathcal{P}_n \setminus \{\overline{\overline{(a_i, b_j)}}\} \tag{10}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\widetilde{C}_n = \langle v^{\widetilde{(a_i,b_j)}} \mid (a_i, b_j) \in \mathcal{P}_n \rangle. \tag{11}$$

Finally, from the reflexive graph $\widetilde{L}_n^R$ we get a 1-$(n^2, n^2-2n+2, n^2-2n+2)$ design $\widetilde{\widetilde{\mathcal{D}}}_n$ (for $n \geq 3$) with blocks

$$\widetilde{\widetilde{(a_i, b_j)}} = \widetilde{(a_i, b_j)} \cup \{(a_i, b_j)\} \tag{12}$$

for each point $(a_i, b_j) \in \mathcal{P}_n$, and p-ary code

$$\widetilde{\widetilde{C}}_n = \langle v^{\widetilde{\widetilde{(a_i,b_j)}}} \mid (a_i, b_j) \in \mathcal{P}_n \rangle. \tag{13}$$

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

$$v^{\overline{\overline{(a,b)}}} + v^{\widetilde{(a,b)}} = \boldsymbol{\jmath} = v^{\overline{(a,b)}} + v^{\widetilde{\widetilde{(a,b)}}}. \tag{14}$$

The group $G = S_n \wr S_2$ is the automorphism group of $K_{n,n}$. It acts on the edge set $\mathcal{P}_n = A \times B$ by its construction as an extension of the group $H = S_n \times S_n$ by $S_2 = \{1, \tau\}$, where $\tau = (1, 2)$. The element τ then acts on H via $(\alpha, \beta)^\tau = (\beta, \alpha)$, for $\alpha, \beta \in S_n$. Then G acts as a rank-3 group on $\mathcal{P}_n$ as follows:

$$(a_i, b_j)^{(\alpha,\beta)} = (a_{i^\alpha}, b_{j^\beta}), \text{ and } (a_i, b_j)^\tau = (a_j, b_i). \tag{15}$$

Furthermore, G 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 obtain now the basic properties of $C_n = C_p(\mathcal{G}_n) = C_p(M_n)$. We first need a lemma. The notation is as established in the last section.

Lemma 1 *For $n \geq 2$, if $\{i, j, k, m\} \subseteq \Omega$ where $i \neq k$, and $j \neq m$, then the vector*

$$u = u((a_i, b_j), (a_k, b_m)) = v^{(a_i,b_j)} + v^{(a_k,b_m)} - v^{(a_i,b_m)} - v^{(a_k,b_j)} \tag{16}$$

is in $C_n^{\perp}$.

Proof: This is clear since $(\overline{x}, u) = 0$ for all choices of $x \in A \cup B$. ■

Proposition 1 *For $n \geq 2$, the code C_n over $\mathbb{F}_p$ of the incidence design $\mathcal{G}_n$ of the complete bipartite graph $K_{n,n}$ is a $[n^2, 2n-1, n]_p$ code. For $n \geq 3$, the minimum-weight vectors are the scalar multiples of the incidence vectors of the blocks of $\mathcal{G}_n$.*

Proof: It is easy to see that the matrix M_n has rank $2n-1$ over any field, and that the minimum weight is at most n.

Now let $\mathcal{B}_n$ be the set of supports of the vectors $u((a_i, b_j), (a_k, b_m))$ as defined in Equation (16). Then $(\mathcal{P}_n, \mathcal{B}_n)$ is a 1-$(n^2, 4, r)$ design, where $r = (n-1)^2$.

Let $w \in C_n$ and $\mathrm{Supp}(w) = \mathcal{S}$, 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 $P = (a_i, b_j)$. Then

1. if $Q = (a_i, b_k)$ then $P, Q \in \mathrm{Supp}(u((a_i, b_j), (a_m, b_k))$ for all $m \neq i$, giving $n-1$ such blocks;
2. if $Q = (a_m, b_j)$ then P, Q are on $n-1$ blocks again;
3. if $Q = (a_m, b_k)$ where $m \neq i, k \neq j$, then $P, Q \in \mathrm{Supp}(u((a_i, b_j), (a_m, b_k))$ only, giving one block.

Suppose that in $\mathcal{S}$ there are k points of the type (a_i, b_k) or (a_m, b_j), and ℓ of the type (a_m, b_k) where $m \neq i, k \neq j$. 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 $z_2 + 2z_3 + 3z_4 = (n-1)k + \ell = (n-1)(s-\ell-1) + \ell = (n-1)(s-1) - \ell(n-2)$. Thus $r = (n-1)^2 \leq (n-1)(s-1) - \ell(n-2) \leq (n-1)(s-1)$ for $n \geq 2$. So $s \geq n$ for $n \geq 2$, giving the minimum weight as stated.

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

Note: For $n = 2$ there are words of weight 2 in C_n for all odd p that are not scalar multiples of the incidence vectors of the blocks of $\mathcal{G}_n$, *viz.*, for example, $w = \jmath - v^{\overline{a_1}} - v^{\overline{b_1}}$.

Proposition 2 *For $n \geq 2$, and $C_n = C_p(\mathcal{G}_n)$,*

$$\mathcal{U} = \{u((a_i, b_j), (a_{i+1}, b_{j+1})) \mid 1 \leq i \leq n-1, 1 \leq j \leq n-1\}$$

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

Proof: We consider $\mathcal{U}$ as a sequence ordered first through fixing i, and allowing j to take the values 1 to $n-1$ within each fixed i. Thus the sequence is

$$[u((a_1, b_1), (a_2, b_2)), u((a_1, b_2), (a_2, b_3), \ldots, u((a_{n-1}, b_{n-1}), (a_n, b_n))].$$

If the points of $\mathcal{P}_n$ are ordered as described for M_n in Equation (1), then the array of vectors from $\mathcal{U}$ is in echelon form. Since $|\mathcal{U}| = (n-1)^2 = n^2 - (2n-1) = \dim(C_n^{\perp})$, we have the result. ■

Proposition 3 *For $n \geq 3$, and $C_n = C_p(\mathcal{G}_n)$, $\mathrm{Aut}(\mathcal{G}_n) = \mathrm{Aut}(C_n) = S_n \wr S_2$.*

Proof: From Whitney's theorem [24] it is clear that $\mathrm{Aut}(L_n) = \mathrm{Aut}(K_{n,n}) = S_n \wr S_2$ and thus $S_n \wr S_2 \subseteq \mathrm{Aut}(\mathcal{G}_n)$. For the reverse inclusion, suppose that $\sigma \in \mathrm{Aut}(\mathcal{G}_n)$. To show that $\sigma \in \mathrm{Aut}(L_n)$, suppose P and Q are adjacent in L_n. Then $P = (a_i, b_j)$ and $Q = (a_i, b_k)$ or (a_k, b_j), so $P, Q \in \overline{a_i}$ or $\overline{b_j}$. Thus $P\sigma, Q\sigma \in \overline{x}$ for some $x \in A \cup B$, and so $P\sigma$ and $Q\sigma$ are adjacent in L_n and hence $\sigma \in \mathrm{Aut}(L_n)$.

For $n \geq 3$, by Proposition 1, the words of weight n 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 $\sigma \in \mathrm{Aut}(\mathcal{G}_n) = S_n \wr S_2$, and thus $\mathrm{Aut}(C_n) = S_n \wr S_2$ for $n \geq 3$. ■

Proposition 4 *For $n \geq 3$, and $C_n = C_p(\mathcal{G}_n)$,*

$$\mathcal{I}_n = \{(a_i, b_n) \mid 1 \leq i \leq n\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n-1\}$$

is an information set for C_n and the set

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

of elements of $S_n \times S_n$, is a PD-set for C_n of size n for the information set $\mathcal{I}_n$.

Proof: That $\mathcal{I}_n$ is an information set follows from Proposition 2. Let $\mathcal{C}_n$ be the corresponding check set. To prove that S is a PD-set for C_n, note that C_n can correct $t = \lfloor \frac{n-1}{2} \rfloor$ errors. Let

$$\mathcal{T} = \{(a_{i_1}, b_{j_i}), \ldots, (a_{i_t}, b_{j_t})\}$$

be a set of t points of $\mathcal{P}_n$, and $\Omega_1 = \{i_1, \ldots, i_t\}$, $\Omega_2 = \{j_1, \ldots, j_t\}$, $\mathcal{O} = \Omega_1 \cup \Omega_2$. Then since $t \leq \frac{n-1}{2}$, $|\mathcal{O}| \leq 2t \leq n-1$. If $n \notin \mathcal{O}$ then we use the identity ι. If $n \in \mathcal{O}$ then there is a $k \in \Omega$, $k \neq n$, such that $k \notin \mathcal{O}$ and the element $(t_{n,k}, t_{n,k})$ will move $\mathcal{T}$ into $\mathcal{C}_n$. Thus we have a PD-set. ■

Note: Result 1 gives the bounds $\frac{n}{2}$ for n even, and $\frac{n+3}{2}$ for n odd for the smallest size possible for a PD-set. Our set has size n.

Recall that the code E_n is defined in Equation (5).

Proposition 5 *For $n \geq 3$, let $E_n = \langle v^{\overline{x}} - v^{\overline{y}} \mid x, y \in A \cup B \rangle$ over $\mathbb{F}_p$. Then E_n is a $[n^2, 2n-2, 2n-2]_p$ code and the words of weight $2n-2$ are the scalar multiples of $v^{\overline{a_i}} - v^{\overline{b_j}}$, for $1 \leq i, j \leq n$.*

Proof: It is clear that $E_n = \langle v^{\overline{x}} - v^{\overline{a_1}} \mid x \in A \cup B \rangle$ and has codimension at most 1 in C_n. In C_n we have $\sum_{i=1}^n v^{\overline{a_i}} = \sum_{i=1}^n v^{\overline{b_i}} = \boldsymbol{j}$, and so $\sum_{i=1}^n (v^{\overline{a_i}} - v^{\overline{a_1}}) = \sum_{i=1}^n (v^{\overline{b_i}} - v^{\overline{a_1}})$, showing that E_n has dimension at most $2n-2$, and thus exactly $2n-2$.

For the minimum weight, $E_n \neq C_n$ so if $w \in E_n$ and $w \neq 0$, it must follow that $\mathrm{wt}(w) \geq n+1$, since the words of weight n in C_n are the scalar multiples of the $v^{\overline{x}}$, for $x \in A \cup B$. Further, $\mathrm{wt}(v^{\overline{x}} - v^{\overline{y}}) = 2(n-1)$. Suppose $\mathrm{wt}(w) = n + j = s$ where $1 \leq j \leq n-3$, and show we have a contradiction. Let $\mathcal{S} = \mathrm{Supp}(w)$. Count as in Proposition 1, considering intersections of $\mathcal{S}$ with weight-4 vectors in $C_n^\perp \subset E_n^\perp$.

For $P = (a_1, b_1) \in \mathcal{S}$ let

- $K_P = \{Q \mid Q \in \mathcal{S}, Q = (a_1, b_j) \text{ or } (a_k, b_1), j, k \neq 1\}$, $k_P = |K_P|$;
- $L_P = \{Q \mid Q \in \mathcal{S}, Q = (a_j, b_k), j, k \neq 1\}$, $\ell_P = |L_P|$.

If $Q \in L_P$, $Q = (a_2, b_2)$ say, then $K_P \cap K_Q \subseteq \{(a_1, b_2), (a_2, b_1)\}$, so $|K_P \cap K_Q| \leq 2$.

We have $s = |\mathcal{S}| = n + j = k_P + \ell_P + 1$ for any $P \in \mathcal{S}$. Fix some $P \in \mathcal{S}$ and write $k = k_P$ and $\ell = \ell_P$. Counting as in Proposition 1, we get

$$(n-1)^2 \leq (n-1)k + \ell = (n-1)(n+j-1-\ell) + \ell = (n-1)^2 + (n-1)j - \ell(n-2),$$

which gives

$$\ell \leq \frac{(n-1)j}{(n-2)} \quad \text{and} \quad k \geq n - 1 - \frac{j}{n-2}. \tag{17}$$

We remark that if $\ell_P = 0$ for $P = (a_1, b_1)$, then $\mathcal{S} = K_P \cup \{P\}$. Since $s \geq n+1$, by assumption, $k_P \geq n \geq 2$, K_P must contain points of the form (a_1, b_j) and (a_k, b_1), $k, j \neq 1$ and thus we can always find two points P and Q such that $Q \in L_P$, and then also $P \in L_Q$.

So suppose $Q \in L_P$. Then $|K_P \cap K_Q| = t \leq 2$. Since also then $P \in L_Q$, we get that $|K_P \cup K_Q| = k_P + k_Q - t$. Thus

$$s = n + j \geq k_P + k_Q - t + 2 = (n + j - 1 - \ell_P) + (n + j - 1 - \ell_Q) - t + 2,$$

so that

$$\ell_P + \ell_Q \geq n + j - t.$$

Together with Equation (17) for $\ell = \ell_P, \ell_Q$, this implies $2(n-1)j \geq (n+j-t)(n-2)$ and hence

$$j \geq n - (t+2) + \frac{2t}{n}. \tag{18}$$

If $t = 2$ we get $j \geq n-3$, and if $t = 1$ or $t = 0$ we get $j \geq n-2$ or $n-1$ respectively, which is impossible since $j \leq n-3$. Thus we must have $j = n-3$, $s = 2n-3$ and $k \geq n - 1 - \frac{n-3}{n-2}$, so $k \geq n-1$ for all points. But if $t = 2$ then $s = 2n-3 = 2(n-3)+2+2 = 2n-2$, which is impossible. So there are no words of C_n in this range, and the minimum weight of E_n is $2n-2$.

Now to show that the words of weight $2n-2$ are the scalar multiples of the words $v^{\overline{a_i}} - v^{\overline{b_j}}$, we put $s = 2n-2$ in the above argument and obtain $k \geq n-2$ for all points. Again we take P, Q such that $P \in L_Q$, $Q \in L_P$, and we get the following possibilities:

1. $k_P = k_Q = n-1, t = 2$;
2. $k_P = n-2, k_Q = n, t = 2$;
3. $k_P = n-2, k_Q = n-1, t = 1, 2$;
4. $k_P = k_Q = n-2, t = 0, 1, 2$.

We show that the only possibility is the last case with $t = 0$, and that this has to be of the form stated. The main argument used will be that, taking $P = (a_1, b_1)$, $Q = (a_2, b_2)$, the weight-4 word $u((a_1, b_1), (a_k, b_m))$ for $k, m \geq 3$ must meet $\mathcal{S} = \mathrm{Supp}(w)$ again.

Thus in Case (1) we have $\mathcal{S} = K_P \cup K_Q \cup \{P, Q\}$, leaving $n-3$ points available in $K_P \setminus K_Q$, but at least $n-2$ are needed to meet all the weight-4 words. Case (2) is the same, as is Case (3) with $t = 1$. In Case (3) with $t = 2$, $\mathcal{S} = K_P \cup K_Q \cup \{P, Q, R\}$ where $R \in L_P \cap L_Q$. The same argument then eliminates this possibility.

In Case (4), if $t = 2$ there are two more points, both in $L_P \cap L_Q$, and if $t = 1$ there is one more point. In both cases the same argument can be used. This leaves only the Case (4) with $t = 0$. Here there are $(n-2)^2$ words of weight 4 that must meet K_P again and unless $K_P = \overline{a_1} \setminus \{(a_1, b_1), (a_1, b_2)\}$ or $\overline{b_1} \setminus \{(a_1, b_1), (a_2, b_1)\}$ this will not be possible. Similarly for K_Q. If $K_P = \overline{a_1} \setminus \{(a_1, b_1), (a_1, b_2)\}$ and $K_Q = \overline{a_2} \setminus \{(a_2, b_2), (a_2, b_1)\}$ then for $R = (a_1, b_3)$ we have $k_R = n-1$, which we have already shown to be impossible. So $\mathrm{Supp}(w) = \mathrm{Supp}(v^{\overline{a_1}} - v^{\overline{b_2}})$, and, from the intersections with the weight-4 words in $E_n^\perp$, we have $w((a_1, b_1)) = -w((a_2, b_2))$, $w((a_1, b_1)) = w((a_1, b_j))$ for $j \geq 3$ and $w((a_2, b_2)) = w((a_j, b_2))$ for $j \geq 3$. Thus $w = \alpha(v^{\overline{a_1}} - v^{\overline{b_2}})$ for some $\alpha \in \mathbb{F}_p$. ■

Proposition 6 *For $n \geq 3$, let $E_n = \langle v^{\overline{x}} - v^{\overline{y}} \mid x, y \in A \cup B \rangle$. Then*

$$\mathcal{I}_n^* = \{(a_i, b_n) \mid 1 \leq i \leq n\} \cup \{(a_n, b_i) \mid 1 \leq i \leq n-1\} \setminus \{(a_1, b_n)\}$$

is an information set for E_n and

$$S = \{(t_{n,i}, t_{n,j}) \mid 1 \leq i, j \leq n\}, \tag{19}$$

of elements of $S_n \times S_n$ is a PD-set of size n^2 for E_n using $\mathcal{I}_n^*$.

Proof: That $\mathcal{I}_n^*$ is an information set follows from Proposition 2. Let $\mathcal{C}_n$ be the corresponding check set. To prove that S is a PD-set for E_n, note that E_n can correct $n-2$ errors. Let

$$\mathcal{T} = \{(a_{i_1}, b_{j_i}), \ldots, (a_{i_t}, b_{j_t})\}$$

be a set of $t \leq n-2$ points of $\mathcal{P}_n$, and $\Omega_1 = \{i_1, \ldots, i_t\}$, $\Omega_2 = \{j_1, \ldots, j_t\}$, $\mathcal{O} = \Omega_1 \cup \Omega_2$. If $n \notin \mathcal{O}$ then we use the identity ι. Since $t \leq n-2$ there is a $k \neq n$, $k \notin \Omega_1$ and an $\ell \neq n$, $\ell \notin \Omega_2$, and $(t_{n,k}, t_{n,\ell})$ will move $\mathcal{T}$ into $\mathcal{C}_n$. Thus we have a PD-set. ■

Note: This is the same PD-set as was used in the binary case in [16]. In that paper it was shown that Result 1 gives a bound linear in n. Our set has size n^2.

When p divides n, a further class of codes with a larger minimum weight than E_n and correcting $n-1$ errors, can be obtained.

Proposition 7 *If $n \geq 3$, p divides n, and*

$$E_n^* = \langle v^{\overline{a_i}} - v^{\overline{a_1}}, v^{\overline{b_i}} - v^{\overline{b_1}} \mid i \in \{1, \ldots, n\} \rangle,$$

then E_n^* is a self-orthogonal $[n^2, 2n-3, d]_p$ code, where $d = 2n-1$ or $2n$. An information set for E_n^* is $\mathcal{I}_n^* \setminus \{(a_n, b_n)\}$.

If p is odd then $E_n^* = \mathrm{Hull}(E_n)$. If $p = 2$ then $E_n^* \subset \mathrm{Hull}(E_n) = E_n$ and E_n^* is a doubly-even $[n^2, 2n-3, 2n]_2$ code.

Proof: Since $\sum_{i=1}^n (v^{\overline{a_i}} - v^{\overline{a_1}}) = \jmath + nv^{\overline{a_1}}$ and $\sum_{i=1}^n (v^{\overline{b_i}} - v^{\overline{b_1}}) = \jmath + nv^{\overline{b_1}}$, we have

$$\jmath = \sum_{i=1}^n (v^{\overline{a_i}} - v^{\overline{a_1}}) - nv^{\overline{a_1}} = \sum_{i=1}^n (v^{\overline{b_i}} - v^{\overline{b_1}}) - nv^{\overline{b_1}},$$

and so $n(v^{\overline{a_1}} - v^{\overline{b_1}}) \in E_n^*$, so that if $p \not| n$, then $E_n^* = E_n$.

So suppose $p|n$. Then $(v^{\overline{a_i}} - v^{\overline{a_1}}, v^{\overline{x}}) = 0$ for all $x \in A \cup B$, and similarly for $(v^{\overline{b_i}} - v^{\overline{b_1}}, v^{\overline{x}})$, so that $E_n^* \subseteq C_n^\perp \subset E_n^\perp$. But $E_n \not\subseteq C_n^\perp$, so $E_n^* \neq E_n$, $E_n^* \subseteq \mathrm{Hull}(E_n)$ and $[E_n : E_n^*] = 1$. Since $E_n^* \neq E_n$ and has vectors of weight $2n$, its minimum weight is $2n-1$ or $2n$. Also, looking at inner products, we see that with $p|n$ then $E_n \subseteq E_n^\perp$ only if $p = 2$, i.e. $E_n^* = \mathrm{Hull}(E_n)$ if $p \neq 2$, and $\mathrm{Hull}(E_n) = E_n$ if $p = 2$. So if $p = 2$, E_n and E_n^* are self-orthogonal, E_n^* is doubly-even, and hence its minimum weight must be $2n$.

That $\mathcal{I}_n^* \setminus \{(a_n, b_n)\}$ is an information set is clear from the matrix M_n. ■

Corollary 2 *For $n \geq 3$, the set S of Equation (19) is a PD-set for E_n^* for the information set $\mathcal{I}_n^* \setminus \{(a_n, b_n)\}$.*

Proof: The proof is almost identical to that for E_n, except that we are taking a set of size $n-1$. Thus

$$\mathcal{T} = \{(a_{i_1}, b_{j_i}), \ldots, (a_{i_t}, b_{j_t})\}$$

is a set of $t \leq n-1$ points of $\mathcal{P}_n$, and $\Omega_1 = \{i_1, \ldots, i_t\}$, $\Omega_2 = \{j_1, \ldots, j_t\}$, $\mathcal{O} = \Omega_1 \cup \Omega_2$. If $n \notin \mathcal{O}$ then we use the identity ι. So suppose $n \in \mathcal{O}$. If there is a $k \neq n$, $k \notin \Omega_1$ and an $\ell \neq n$, $\ell \notin \Omega_2$, and $(t_{n,k}, t_{n,\ell})$ will move $\mathcal{T}$ into $\mathcal{C}_n$. Otherwise, if $n \in \Omega_1$ and $\Omega_2 = \{1, \ldots, n-1\}$, then there is a $k \notin \Omega_1$, $k \neq n$, and $(t_{k,n}, t_{n,n})$ will map $\mathcal{T}$ into $\mathcal{C}_n$. Thus we have a PD-set. ■

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 from the lattice graph nor its complementary graph, nor from the reflexive graphs, give any interesting new codes beyond the codes C_n and E_n that we have already examined.

We use the notation established in Section 3.

Lemma 2 *For $n \geq 2$, p an odd prime, the weight-4 vectors $u((a_i, b_j), (a_k, b_m))$ of Equation (16) are in all $\overline{C}_n, \overline{\overline{C}}_n, \widetilde{C}_n, \widetilde{\widetilde{C}}_n$. For $p = 2$, $u \in \overline{\overline{C}}_n, \widetilde{C}_n$.*

Proof: It can be verified easily that if $u = u((a_i, b_j), (a_k, b_m))$, then

$$v^{\overline{(a_i,b_j)}} + v^{\overline{(a_k,b_m)}} - v^{\overline{(a_i,b_m)}} - v^{\overline{(a_k,b_j)}} = -2u.$$

It then follows from Equations (8) and (14) that

$$\begin{aligned} v^{\overline{\overline{(a_i,b_j)}}} + v^{\overline{\overline{(a_k,b_m)}}} - v^{\overline{\overline{(a_i,b_m)}}} - v^{\overline{\overline{(a_k,b_j)}}} &= -u \\ v^{\widetilde{(a_i,b_j)}} + v^{\widetilde{(a_k,b_m)}} - v^{\widetilde{(a_i,b_m)}} - v^{\widetilde{(a_k,b_j)}} &= u \\ v^{\widetilde{\widetilde{(a_i,b_j)}}} + v^{\widetilde{\widetilde{(a_k,b_m)}}} - v^{\widetilde{\widetilde{(a_i,b_m)}}} - v^{\widetilde{\widetilde{(a_k,b_j)}}} &= 2u, \end{aligned}$$

which gives the result. ■

Proposition 8 *For $n \geq 2$, p an odd prime,*

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

For $p = 2$, $\overline{C}_n = E_n$; $\overline{\overline{C}}_n = E_n^\perp$ if n is odd, $\overline{\overline{C}}_n = \mathbb{F}_p^{n^2}$ if n is even; $\widetilde{C}_n = C_n^\perp$ if n is odd, $\widetilde{C}_n = \mathbb{F}_p^{n^2}$ if n is even; $\widetilde{\widetilde{C}}_n = E_n$ for n even, $\widetilde{\widetilde{C}}_n = C_n$ for n odd.

Proof: First take p odd. Let $u(1,2) = \sum_{i\neq 1}^n u((a_1, b_1), (a_2, b_i)) = \sum_{i\neq 1}^n (v^{(a_1,b_1)} + v^{(a_2,b_i)} - v^{(a_1,b_i)} - v^{(a_2,b_1)})$. Then it follows that

$$u(1,2) = (n-1)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) - \sum_{i\neq 1} (v^{(a_2,b_i)} - v^{(a_1,b_i)}),$$

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

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

$$\begin{aligned} v^{\overline{(a_1,b_1)}} - v^{\overline{(a_2,b_1)}} &= (n-1)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) - u(1,2) - (v^{(a_1,b_1)} - v^{(a_2,b_1)}) \\ &= (n-2)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) - u(1,2) \end{aligned}$$

   is in $\overline{C}_n$.

   If $n \not\equiv 2 \pmod p$ then $v^{(a_1,b_1)} - v^{(a_2,b_1)} \in \overline{C}_n$, and this will hold for any pairs of points, so $\langle \jmath \rangle^\perp \subseteq \overline{C}_n$. But $\jmath \in \overline{C}_n^\perp$ only if $n \equiv 1 \pmod p$, so we have the stated result for $n \not\equiv 2 \pmod p$.

   If $n \equiv 2 \pmod p$, then since $(v^{\overline{x}}, v^{\overline{(y,z)}}) = 1$ if $x \neq y, z$ and $n-1$ 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 $\overline{\overline{C}}_n$:

$$\begin{aligned} v^{\overline{\overline{(a_1,b_1)}}} - v^{\overline{\overline{(a_2,b_1)}}} &= v^{\overline{(a_1,b_1)}} - v^{\overline{(a_2,b_1)}} + v^{(a_1,b_1)} - v^{(a_2,b_1)} \\ &= (n-1)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) - u(1,2), \end{aligned}$$

from the previous case, is in $\overline{\overline{C}}_n$.

If $n \not\equiv 1 \pmod p$ then $v^{(a_1,b_1)} - v^{(a_2,b_1)} \in \overline{\overline{C}}_n$, 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 $2n \equiv 1 \pmod p$, so we have the stated result for $n \not\equiv 1 \pmod p$.

If $n \equiv 1 \pmod p$, then since $(v^{\overline{x}}, v^{\overline{\overline{(y,z)}}}) = 1$ if $x \neq y, z$ and n 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 $\widetilde{C}_n$:
$v^{\widetilde{(a,b)}} + v^{\overline{\overline{(a,b)}}} = \boldsymbol{\jmath}$, so

$$\begin{aligned} v^{\widetilde{(a_1,b_1)}} - v^{\widetilde{(a_2,b_1)}} &= -v^{\overline{\overline{(a_1,b_1)}}} + v^{\overline{\overline{(a_2,b_1)}}} \\ &= -(n-1)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) + u(1,2), \end{aligned}$$

from the previous case, is in $\widetilde{C}_n$.

If $n \not\equiv 1 \pmod p$ then $v^{(a_1,b_1)} - v^{(a_2,b_1)} \in \widetilde{C}_n$. and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^\perp \subseteq \widetilde{C}_n$. But $\boldsymbol{\jmath} \notin \widetilde{C}_n^\perp$ for $n \not\equiv 1 \pmod p$, so we have the stated result for $n \not\equiv 1 \pmod p$.

If $n \equiv 1 \pmod p$, then since $(v^{\overline{x}}, v^{\widetilde{(y,z)}}) = n - 1$ 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 we have equality.

4. For $\widetilde{\widetilde{C}_n}$:
$v^{\widetilde{\widetilde{(a,b)}}} = v^{\widetilde{(a,b)}} + v^{(a,b)}$, so

$$\begin{aligned} v^{\widetilde{\widetilde{(a_1,b_1)}}} - v^{\widetilde{\widetilde{(a_2,b_1)}}} &= v^{\widetilde{(a_1,b_1)}} - v^{\widetilde{(a_2,b_1)}} + v^{(a_1,b_1)} - v^{(a_2,b_1)} \\ &= -(n-2)(v^{(a_1,b_1)} - v^{(a_2,b_1)}) + u(1,2), \end{aligned}$$

from the previous case, is in $\widetilde{\widetilde{C}_n}$.

If $n \not\equiv 2 \pmod p$ then $v^{(a_1,b_1)} - v^{(a_2,b_1)} \in \widetilde{\widetilde{C}_n}$. and this will hold for any pairs of points, so $\langle \boldsymbol{\jmath} \rangle^\perp \subseteq \widetilde{C}_n$. But $\boldsymbol{\jmath} \notin \widetilde{\widetilde{C}_n}^\perp$ so we have the stated result for $n \not\equiv 2 \pmod p$.

If $n \equiv 2 \pmod p$, then since $(v^{\overline{x}}, v^{\widetilde{\widetilde{(y,z)}}}) = n - 1$ 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 for p odd.

Now take $p = 2$. That $\overline{C}_n = E_n$ follows from the observation that $M_n^T M_n = A_n$ (in the notation of Section 3), or from Result 2.

For $\overline{\overline{C}}_n$, from Lemma 2, $u(1,2) \in \overline{\overline{C}}_n$, and the same argument as in the case of odd p can be used; similarly for $\widetilde{C}_n$.

For $\widetilde{\widetilde{C}}_n$, since $v^{\widetilde{(a,b)}} = \jmath + v^{\overline{(a,b)}} = \jmath + v^{\overline{a}} + v^{\overline{b}}$, $\sum_{i=1}^{n} v^{\widetilde{(a_i,b)}} = n\jmath + \sum_{i=1}^{n} v^{\overline{a_i}} + nv^{\overline{b}} = \jmath$ for n even, and equal to $v^{\overline{b}}$ for n odd, and so $\widetilde{\widetilde{C}}_n = C_n$ for n odd. For n even, $\sum_{i=1}^{n} v^{\overline{(a_i,b)}} = \jmath$, so for n even, $\widetilde{\widetilde{C}}_n = \overline{C}_n = E_n$.

This completes the proof of all the cases. ■

The proof of Theorem 1 now follows from the results in this and the last section.

Acknowledgement

The authors thank the Department of Mathematics and Applied Mathematics at the University of the Western Cape for their hospitality.

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] W. Fish, J. D. Key, and E. Mwambene. Binary codes of line graphs from the n-cube. *J. Symbolic Comput.*, 45:800–812, 2010.

[7] W. Fish, J. D. Key, and E. Mwambene. Codes from the incidence matrices and line graphs of Hamming graphs. *Discrete Math.*, 310:1884–1897, 2010.

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

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

[10] 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.

[11] 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.

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

[13] J. D. Key, J. Moori, and B. G. Rodrigues. Codes associated with triangular graphs, and permutation decoding. *Int. J. Information and Coding Theory*, 1, No.3:334–349, 2010.

[14] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*, 28:121–126, 2006.

[15] J. D. Key and P. Seneviratne. Codes from the line graphs of complete multipartite graphs and PD-sets. *Discrete Math.*, 307:2217–2225, 2007.

[16] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.*, 308:2862–2867, 2008.

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

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

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

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

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

[22] Padmapani Seneviratne. *Permutation decoding of codes from graphs and designs.* PhD thesis, Clemson University, 2007.

[23] 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.

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