Codes from the line graphs of complete multipartite graphs and PD-sets

J. D. Key [a,*,1] P. Seneviratne [a]

[a] *Department of Mathematical Sciences, Clemson University, Clemson SC 29634, U.S.A.*

Abstract

The binary codes of the line graphs $L_m(n)$ of the complete multipartite graphs $K_{n_1,\ldots,n_m}$ ($n_i = n$ for $1 \leq i \leq m$) $n \geq 2$, $m \geq 3$ are examined, and PD-sets and s-PD-sets are found.

Key words: Codes, graphs, designs
PACS: 05, 51, 94

1 Introduction

We consider the binary codes of the line graphs $L_m(n)$ of the complete multipartite graphs $K_{n,\ldots,n}$ as candidates to which permutation decoding can be applied, i.e. PD-sets (for full error-correction) or s-PD-sets (for correcting s errors, see Definition 1, Section 2) can be found. Since the automorphism group of $L_m(n)$ and of its binary code is the wreath product $S_n \wr S_m$ (where S_r denotes the symmetric group of degree r) it can be expected that information sets can be found for permutation decoding, as was done for some other classes of codes from graphs with a great deal of symmetry: see [8,9,11,10]. We have found PD-sets for some classes and s-PD-sets for all the classes. Our main results are summarized in the following theorem, where the notation for the points of the information set is defined in Equation 1, Section 2, and where we take $m \geq 3$, since $m = 2$ has been considered earlier in [11,10]:

* Corresponding author.

[1] This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565.

Theorem 1 *If C is the binary code of the line graph $L_m(n)$ of the complete multipartite graph $K_{n,\ldots,n}$ of nm vertices, where $n \geq 2$, $m \geq 3$, then*

- *C is a $[\,\frac{1}{2}m(m-1)n^2, mn-2, 2n(m-1)-2\,]_2$ code for mn even;*
- *C is a $[\,\frac{1}{2}m(m-1)n^2, mn-1, n(m-1)\,]_2$ code for mn odd.*

Let $\mathcal{I}$ be the set

$$\{(1,1:i,j) \mid 2 \leq i \leq m, 1 \leq j \leq n\} \cup \{(1,i:2,1) \mid 2 \leq i \leq n\} \setminus \{(1,1:m,n)\}$$

and $\mathcal{I}^* = \mathcal{I} \cup \{(1,2:m,n)\}$. Then $\mathcal{I}$ is an information set for C if mn is even, and $\mathcal{I}^*$ is an information set for mn odd. Using these information sets

(1) if $n = 2$ and $m \geq 3$, C has a PD-set of size $16m^2 - 8m$;
(2) if $n = 3$ and $m \geq 3$ is odd, C has a PD-set of size $27m$;
(3) if $m = 3$ and $n \geq 3$ is odd, C has a PD-set of size $2n^3$.

Furthermore, s-PD-sets of size N exist as follows: $s < m/2$, $N = m$; $s < m$, $N = mn^2$; $s < 3m/2$, $N = mn^3$; $s < 2m$, mn even, $N = 4m^2n^2 - 2mn^2$; $s < n/2$, $N = n$ for mn even, $N = 2n$ for mn odd; $s < n$, $N = n^3$ for mn even, $N = 2n^3$ for mn odd.

The parts of this theorem are proved, and the explicit PD-sets or s-PD-sets are given, in the following sections as Propositions 1, 2, 4, 5, 6, 7 and Corollaries 2 and 3. Also note that these sizes are not necessarily the best, and in most explicit cases, smaller ones can be found with Magma [2]. It is also assumed that one only considers using s-PD-sets if $s \leq t$, where t is the full error-correction cabability of the code.

In [6,7,5] it is shown that as the parameters for the designs and codes increase, PD-sets for full error correction cannot be found for some classes if the automorphism group does not grow fast enough with the parameters. This was shown using the bound for the smallest size of a PD-set from Result 2. In those papers designs from geometries and Paley graphs were examined and small s-PD-sets were found for partial permutation decoding.

The paper is arranged as follows: in Section 2 the basic notation and definitions, including those for permutation decoding, are given; in Section 3 the main parameters of the codes are established; in Section 4 the PD-sets are found.

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 C_F 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 $v^{\mathcal{Q}}$. If $\mathcal{Q} = \{P\}$ where $P \in \mathcal{P}$, then we will write v^P instead of the more cumbersome $v^{\{P\}}$. Thus $C_F = \left\langle v^B \,|\, B \in \mathcal{B} \right\rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

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 of a vector 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 **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 first k coordinates 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. A graph is **regular** if all the vertices have the same valency. The **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. The **p-rank** of the matrix A, denoted by $rank_p(A)$, is the dimension of the row space of A over $\mathbb{F}_p$, the finite field of p elements.

Let $K_{n_1,\ldots,n_m}$ denote the complete multipartite graph on m components. If $n_i = n \geq 2$, for $1 \leq i \leq m$, where $m \geq 3$, then denote the graph by K_n^m. The vertices of K_n^m correspond to the ordered pairs (i, j) for $1 \leq i \leq m$ and $1 \leq j \leq n$, which is the j^{th} point on the i^{th} component, Λ_i. The **line graph** $L_m(n)$ of K_n^m has for vertices the edges of K_n^m and two vertices $L_m(n)$ are adjacent if as edges of K_n^m they had a vertex in common. We will use the

following compact notation for the vertices (points) of $L_m(n)$:

$$\{(i,j),(k,r)\} = (i,j:k,r) = (k,r:i,j). \tag{1}$$

Let $\mathcal{P}$ denote the set of all vertices of $L_m(n)$. The symmetric 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ defined from $L_m(n)$ by taking the vertices as point set $\mathcal{P}$ and defining a block $B = \bar{P}$ for each point P as consisting of the vertices adjacent to that point, i.e.

$$\overline{(a,b:c,d)} = \{(a,b:e,f) \mid (e,f) \neq (c,d)\} \cup \{(c,d:e,f) \mid (e,f) \neq (a,b)\},$$

is a

$$1 - (\frac{1}{2}m(m-1)n^2, 2n(m-1)-2, 2n(m-1)-2)$$

design. The binary code of $\mathcal{D}$ is $C_{\mathbb{F}_2}(\mathcal{D}) = \langle v^B \mid B \in \mathcal{B} \rangle$ where the incidence vector of $B = \overline{(a,b:c,d)}$ is given by

$$v^{\overline{(a,b:c,d)}} = \sum_{(e,f),\, e \neq a} v^{(a,b:e,f)} + \sum_{(e,f),\, e \neq c} v^{(c,d:e,f)}$$

of weight $2n(m-1)-2$.

Permutation decoding was first developed by MacWilliams [12] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [13, Chapter 16, p. 513] and Huffman [4, Section 8]. In [6] 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 $\mathcal{C}$.*

That a PD-set will fully use the error-correction potential of the code follows easily and is proved in Huffman [4, Theorem 8.1]. That an s-PD-set will correct s errors follows in the same way (see [6, Result 2.3]):

Result 1 *Let C be an $[n,k,d]_q$ t-error-correcting code. Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the redundancy positions. Let $y = c + e$ be a vector, where $c \in C$ and e has weight $s \leq t$. Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is $\leq s$.*

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n,k,d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [-A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most s errors occur, where $s \leq t$. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be an s-PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, m$ until an i is found such that the weight of this vector is s or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Such sets might not exist at all, and the property of having a PD-set need not be invariant under isomorphism of codes, i.e. it depends on the choice of $\mathcal{I}$ and $\mathcal{C}$. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [3], from a formula due to Schönheim [14], and quoted and proved in [4]:

Result 2 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$ code C, and $r = n-k$, then*

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

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

A simple argument yields that the worst-case time complexity for the decoding algorithm using an s-PD-set of size z on a code of length n and dimension k is $\mathcal{O}(nkz)$.

3 The binary codes

In this section we obtain the basic results about the binary codes of the graphs $L_m(n)$, starting with the dimension of the codes:

Proposition 1 *Let C be the binary code of $L_m(n)$ where $n \geq 2$ and $m \geq 3$. Then C has dimension $mn-1$ if mn is odd, and dimension $mn-2$ if mn is even.*

PROOF. Let M be a vertex-edge incidence matrix for K_n^m. Then $M^T M = A$ is an adjacency matrix for $L_m(n)$. Thus C is the row span of A over $\mathbb{F}_2$, and clearly C is a subcode of C_M, the row span of M. M has mn rows and each column has two entries. Thus the sum of all the rows is the zero vector, and the rank of C_M is at most $mn-1$.

Order the vertices (rows) and edges (columns) of K_n^m as follows: for the vertices, take the m components in turn, that is, calling these Λ_i for $i = 1$ to m, take $\Lambda_1, \Lambda_2, \ldots, \Lambda_m$. For the edges, take all the edges through the first point in Λ_1, then all the edges through the second point on Λ_1, and so on. Then take the remaining edges through the first point on Λ_2, then the second point on Λ_2, and so on. (See the illustration of this for $m = n = 3$ at the end of the proof.) From this form of M, it is evident that it has rank $mn - 1$ over $\mathbb{F}_2$. (This also follows from Proposition 2.) Thus $\dim C \leq mn - 1$.

Let V be the row span of M^T over $\mathbb{F}_2$. Then $\dim V = mn - 1$. The map $\tau : V \to C$ is defined by $\tau : v = (v_1, \ldots, v_{mn}) \mapsto (v_1, \ldots, v_{mn})M$, so that $V\tau = C$ and $\dim C + \dim \ker(\tau) = \dim V = mn - 1$. A vector v is in the kernel if and only if $v \in V$ and $vM = \mathbf{0}$. Since $\boldsymbol{\jmath} M = \mathbf{0}$, and the null space of M is thus $\langle \boldsymbol{\jmath} \rangle$, we need determine when $\boldsymbol{\jmath} \in V$.

Clearly V is spanned by vectors of weight 2, so V is an even weight code. Thus if mn is odd then $\boldsymbol{\jmath} \notin V$, and $\dim C = mn - 1$. From the form of M^T as described above, and sinceeach vertex of K_n^m is adjacent to $n(m-1)$ vertices, the number of entries in each column is $n(m-1)$. Adding all the rows will give $\boldsymbol{\jmath}$ if $n(m-1)$ is odd, i.e. if n is odd and m is even. Thus in this case $\dim C = mn - 2$. If n is even then if P is a point in the i^{th} component Λ_i, adding all the rows (edges) corresponding to edges through P and the points of Λ_j will give the incidence vector v^{Λ_j} of weight n. Thus $\boldsymbol{\jmath} = \sum_{i=1}^{m} v^{\Lambda_i} \in V$, and $\dim C = mn - 2$. ■

We give an illustration for M for $m = n = 3$, where $\Lambda_i = \{(i,1), (i,2), (i,3)\}$ for $i = 1, 2, 3$:

$$\left[\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
1&1&1&1&1&1& & & & & & & & & & & & \\
 & & & & & &1&1&1&1&1&1& & & & & & \\
 & & & & & & & & & & & & & & & & & \\
\hline
1& & & & & &1& & & & & &1&1&1& & & \\
 &1& & & & & & &1& & & & & & &1&1&1 \\
 & &1& & & & & & &1& & & & & & & & \\
\hline
 & & &1& & & &1& & & &1& &1& &1& &1 \\
 & & & &1& & & &1& & &1& &1& &1& & \\
 & & & & &1& & & &1& & &1& &1& & &1
\end{array}\right]$$

We need the following lemma in order to find information sets for the codes:

Lemma 1 *Let $A_\ell = I_\ell + J_\ell$ with entries in $\mathbb{F}_2$, where $\ell \geq 1$, I_ℓ and J_ℓ are the $\ell \times \ell$ identity and all-one matrices, respectively. For any positive integers j and k let*

$$M_{\ell,k} = \left[\begin{array}{ccc|c} & & & 1 \ldots 1 \\ & A_\ell & & 0 \ldots 0 \\ & & & \vdots \ \vdots \ \vdots \\ & & & 0 \ldots 0 \\ \hline 1 & 0 & \ldots 0 & \\ 1 & 0 & \ldots 0 & A_k \\ \vdots & \vdots & \vdots \ \vdots & \\ 1 & 0 & \ldots 0 & \end{array}\right] \quad \text{and } M^*_{\ell,k} = \left[\begin{array}{ccc|ccc|c} & & & & 1 \ldots & 1 & 0 \\ & A_\ell & & & 0 \ldots & 0 & 0 \\ & & & & \vdots \ \vdots & \vdots & \vdots \\ & & & & 0 \ldots & 0 & 0 \\ \hline 1 & 0 & \ldots 0 & & & & 1 \\ 1 & 0 & \ldots 0 & & A_k & & 0 \\ \vdots & \vdots & \vdots \ \vdots & & & & \vdots \\ 1 & 0 & \ldots 0 & & & & 0 \\ \hline 0 & 0 & \ldots 0 & 1 & 0 & \ldots & 0 \end{array}\right].$$

If ℓ and k are both even or both odd then $\det M_{\ell,k} = 1$. *Furthermore,* $\det M^*_{\ell,k} = \det M_{\ell,k-1}$.

PROOF. Notice that $\det A_\ell = 1$ for ℓ even and that for ℓ and k both even $\det M_{\ell,k} = \det A_\ell \det A_k = 1$. Simple row and column manipulation lead to the remaining results. ■

We use this lemma to establish the information sets for the codes:

Proposition 2 *Let C be the binary code of the graph $L_m(n)$ where $n \geq 2$ and $m \geq 3$. Let $\mathcal{I}$ be the set*

$$\{(1,1:i,j) \mid 2 \leq i \leq m, 1 \leq j \leq n\} \cup \{(1,i:2,1) \mid 2 \leq i \leq n\} \setminus \{(1,1:m,n)\}$$

and $\mathcal{I}^* = \mathcal{I} \cup \{(1,2:m,n)\}$. Then $\mathcal{I}$ is an information set for C if mn is even, and $\mathcal{I}^*$ is an information set for mn odd.

PROOF. Arrange the vertices (points) of an adjacency matrix for $L_m(n)$ in the following order:

$$(1,1:2,1), (1,1:2,2), \ldots, (1,1:2,n), (1,1:3,1), \ldots, (1,1:m,n-1)$$

followed by

$$(1,2:2,1), (1,3:2,1), \ldots, (1,n:2,1), (1,2:m,n),$$

and any ordering for the remaining points. Writing $\ell = mn - n - 1$ and $k = n - 1$, so that $\ell + k + 1 = mn - 1$, the upper left square $mn - 1 \times mn - 1$ part of the adjacency matrix has the form $M^*_{\ell,k}$ of the lemma. We need to show that if mn is even, then $\det M_{\ell,k} = 1$ and if mn is odd then $\det M^*_{\ell,k} = 1$.

If mn is even, then if n is even, $\ell = mn - n - 1$ is odd, and $k = n - 1$ is odd, so by the lemma, $\det M_{\ell,k} = 1$. If mn is even and n is odd, then $\ell = mn - n - 1$ is even and $k = n - 1$ is even and again we have $\det M_{\ell,k} = 1$.

If mn is odd then both n and m are odd, and ℓ is odd. Then $\det M^*_{\ell,k} = \det M_{\ell,k-1} = 1$ since ℓ and $k - 1$ are odd. This proves that $\mathcal{I}$ or $\mathcal{I}^*$ are information sets. ■

As an example, if $m = n = 3$ then $\ell = 5$ and $k = 2$ and ordering the vertices $(1,1:2,1), (1,1:2,2), (1,1:2,3), (1,2:3,1), (1,1:3,2), (1,2:2,1), (1,3:2,1), (1,2:3,3)$, the top 8×8 part of the adjacency matrix is

$$M^*_{5,2} = \left[\begin{array}{ccccc|cc|c} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right].$$

We now find the minimum weight of the codes, and look first at the dual code.

Proposition 3 *Let C be the binary code of $L_m(n)$ for $n \geq 2$, $m \geq 3$. Then $C^\perp$ contains all vectors of the form $v^{\{P,Q,R\}}$ where $P = (a, b : c, d)$, $Q = (c, d : e, f)$ and $R = (a, b : e, f)$ and has minimum weight 3.*

PROOF. Let $w = v^{\{(a,b:c,d),(c,d:e,f),(a,b:e,f)\}} = w(a, b; c, d; e, f)$. We need to show that $\langle w, v^B \rangle = 0$ for all blocks B. Suppose $B = \overline{(a, b : c, d)}$. Then it is clear that v^B meets w twice. Similarly for the other points of w. If $B = \overline{(a, b : x, y)}$ where $(x, y) \neq (c, d), (e, f)$, then again it meets twice. Any block $\overline{(x, y : r, t)}$ where (x, y) and (r, t) are none of $(a, b), (c, d), (e, f)$, will not meet w at all. This completes all the cases. That there can be no vectors of smaller weight follows from an easy argument. ■

Note: The words of weight 3 in the dual code of C are precisely as described in the proposition, except for the case $n = 2$ and $m = 3$, when extra words of weight 3 are present, e.g. $v^{\{(1,1:2,2),(1,2:3,2),(2,1:3,1)\}}$.

We will use the notation

$$w(a,b;c,d;e,f) = v^{\{(a,b:c,d),(c,d:e,f),(a,b:e,f)\}} = v^{(a,b:c,d)} + v^{(c,d:e,f)} + v^{(a,b:e,f)}. \quad (2)$$

Lemma 2 *Any vector of $\mathbb{F}_2^v$, where $v = \frac{1}{2}m(m-1)n^2$, that is orthogonal to every vector $w(a,b;c,d;e,f)$ has weight at least $n(m-1)$.*

PROOF. Let w be a non-zero word of $\mathbb{F}_2^v$ and, without loss of generality, let $P = (1,1:2,1)$ be in the support of w. Every $w(1,1;2,1;x,y)$ for $x \geq 3$ must meet w again, and thus w has at least another $n(m-2)$ points in its support. Either $(1,1:3,1)$ or $(2,1:3,1)$ must be in the support, and thus by the same argument $w(1,1;3,1;2,a)$ or $w(2,1;3,1;1,a)$, $a \neq 1$, must meet w again, yielding a further $n-1$ points of the form $(1,a:3,1)$ or $(2,a:3,1)$, $a \neq 1$, that are not already counted. Thus we get at least $1+n(m-2)+n-1 = n(m-1)$ for the weight of w. ■

Proposition 4 *If C is the binary code of $L_m(n)$, $n \geq 2$, $m \geq 3$, then C has minimum weight $n(m-1)$ if mn is odd, and $2n(m-1)-2$ if mn is even.*

PROOF. If mn is odd then $C = C_M$, where M is the vertex/edge matrix of the graph K_n^m as described in Proposition 1. Every row of M has weight $n(m-1)$, the valency of K_n^m, yielding thus minimum words of C.

For mn even, C has codimension 2 in C_M and is spanned by the the sums of rows of M corresponding to adjacent vertices. The vector w described in Lemma 2 has support at positions $(1,1:x,y)$ or $(2,1:r,s)$, where $x \neq 1, r \neq 2$, and since $w + v^{\overline{(1,1:2,1)}} \in C_M$, $w = \sum_{(x,y),x\neq 1} v^{(1,1:x,y)}$ or $w = \sum_{(x,y),x\neq 2} v^{(2,1:x,y)}$, and thus be the row of M corresponding to the vertex $(1,1)$ or $(2,1)$ of K_n^m. This shows that in the even case, since $C \subset C_M$, the minimum weight is the block size, i.e. the valency of $L_m(n)$, viz. $2n(m-1)-2$. ■

Note: In the mn even case the code is spanned by minimum weight vectors that are incidence vectors, v^B, of blocks of the design.

4 PD-sets

The automorphism group of $L_m(n)$ is the wreath product, $G = S_n \wr S_m$, where S_r denotes the symmetric group of degree r. Thus $G = H \rtimes K$ where $L = S_n \times \ldots \times S_n$, with m terms in the product, and $K = S_m$. Thus G is also an automorphism group of the binary code of $L_m(n)$. We denote the identity element of G by ι, and that of S_n by ι_n, and also, for convenience, use (k, k) (for any integer k) to mean the identity permutation. The action of G on $L_m(n)$ is as follows: for $\tau \in S_m$ and $\sigma = (\sigma_1, \ldots, \sigma_m) \in H$, for $P = (h, i : j, k) \in \mathcal{P}$,

$$P^\tau = (h^{\tau^{-1}}, i : j^{\tau^{-1}}, k),$$

$$P^\sigma = (h, i^{\sigma_h} : j, k^{\sigma_j}),$$

so that $\tau^{-1}\sigma\tau = \sigma^*$, where

$$P^{\sigma^*} = (h, i^{\sigma_{h^\tau}} : j, k^{\sigma_{j^\tau}}).$$

Now we define some special elements of G for our PD-sets:

Definition 2 *Let $G = \mathrm{Aut}(L_m(n)) = H \rtimes K$ where $K = S_m$ and $H = S_n \times \ldots \times S_n$, and $m \geq 3$, $n \geq 2$. The following denote elements of G:*

- $\tau_a^i = (a, i) \in K$ *where* $i, a \in \{1 \ldots m\}$;
- $K^i = \{\tau_a^i \mid 1 \leq a \leq m\} \subseteq K$ *for* $1 \leq i \leq m$;
- $\sigma_b^j \in H$, *where* $\sigma_b^j[j] = (1, b) \in S_n$ *and* $\sigma_b^j[i] = \iota_n$ *for* $i \neq j$, *where* $1 \leq j \leq m$ *and* $1 \leq b \leq n$;
- $H^j = \{\sigma_b^j \mid 1 \leq b \leq n\} \subseteq H$ *for* $1 \leq j \leq m$;
- $\delta_b^j \in H$, *where* $\delta_b^j[j] = (b, n) \in S_n$ *and* $\delta_b^j[i] = \iota_n$ *for* $i \neq j$, *where* $1 \leq j \leq m$ *and* $1 \leq b \leq n$;
- $D^j = \{\delta_b^j \mid 1 \leq b \leq n\} \subseteq H$ *for* $1 \leq j \leq m$;
- $\sigma_a = \prod_{i=1}^m \sigma_a^i = ((1, a), \ldots, (1, a)) \in H$, *for* $1 \leq a \leq n$;
- $H_n = \{\sigma_a \mid 1 \leq a \leq n\} \subseteq H$.

Each of the sets K^i, H^j, D^j, H_n contain the identity ι of G, since we use the notation (a, a), for any a, to denote ι.

For all the following propositions and lemmas we will use the information sets $\mathcal{I}$ and $\mathcal{I}^*$, for mn even or odd, respectively, as found in Proposition 2.

Definition 3 *Let $\mathcal{T} = \{P_i = (a_i, b_i : c_i, d_i) \mid 1 \leq i \leq s\}$ be a set of s points in $\mathcal{P}$, where $a_i \neq c_i$. Let $A = \{a_i, c_i \mid 1 \leq i \leq s\}$ and $B = \{b_i, d_i \mid 1 \leq i \leq s\}$. For $a \in \{1 \ldots m\}$, let $\alpha(a) = |\{P_j \mid a = a_j \text{ or } a = c_j\}|$. Similarly, for $1 \leq j \leq n$, let $\beta(j)$ be the number of times j appears in the b_i and d_i positions in $\mathcal{T}$.*

Lemma 3 *With notation as in Definition* 3 *and* $\mathcal{T}$ *a set of* s *points of* $\mathcal{P}$*, if* $2s \leq km-1$*, (for some integer* k*), then there is an* i *such that* $\alpha(i) \leq k-1$*. If* $2s \leq kn-1$*, (for some integer* k*), then there is a point* j *such that* $\beta(j) \leq k-1$*.*

PROOF. Note that $\sum_{i=1}^{m} \alpha(i) = 2s$ and if $\alpha(i) \geq k$ (for some k) for all $i \in \{1 \dots m\}$, then $2s \geq km$. Thus if $2s \leq km-1$, then there is an i such that $\alpha(i) \leq k-1$. Similarly $\sum_{j=1}^{n} \beta(j) = 2s$. If $\beta(j) \geq k$, where $k \geq 1$, for all j, then $2s \geq kn$. Thus if $2s \leq kn-1$, then there is a point j such that $\beta(j) \leq k-1$. ■

We use this argument in the following propositions.

Proposition 5 *Let* C *be the* $[\,2m(m-1), 2m-2, 4m-6\,]_2$ *code of* $L_m(2)$ *for* $m \geq 3$*, correcting* $t = 2m-4$ *errors. Taking* $\mathcal{I}$ *as information set, a PD-set for* C *is the set of group elements*

$$S = K^1 H^1 (K^2 \cup K^m) H^m \{\iota, \tau_3^2\}$$

of size at most $16m^2 - 8m$*.*

PROOF. Notice first that the points of the information set in this case are

$$\{(1,1:a,1),(1,1:a,2) \mid 2 \leq a \leq m\} \cup \{(1,2:2,1)\} \setminus \{(1,1:m,2).$$

We denote the check set by $\mathcal{C}$. From Lemma 3 we see that for $t = 2m-4$ errors, i.e. $\mathcal{T}$ having t points, there is an i for which $\alpha(i) \leq 3$.

Note that if $\mathcal{T} \subseteq \mathcal{C}$ then ι will take $\mathcal{T}$ to $\mathcal{C}$, and $\iota \in S$ since it is in each of the sets of elements in the definition of S. Every point $P = (a, b : c, d) \in \mathcal{I}$ has $a = 1$ or $c = 1$.

Suppose first there is an i with $\alpha(i) = 0$. If $i = 1$ then $\mathcal{T} \subseteq \mathcal{C}$; if $i \neq 1$ then $\tau_i^1 \in K^1$ will map $\mathcal{T}$ into $\mathcal{C}$, so K^1 will suffice for these t-sets.

Suppose that $\alpha(i) \geq 1$ for all i and that there is an i for which $\alpha(i) = 1$, and thus we take $\alpha(1) = 1$ by using K^1. Then let $P = (1, b; c, d)$ be the only point in $\mathcal{I} \cap \mathcal{T}$. We need to map $\mathcal{T}$ into $\mathcal{C}$. Looking at the cases, if $P = (1, 1 : c, d)$ then σ_2^1 will map P to $P' = (1, 2 : c, d)$ and fix all the other points of $\mathcal{T}$. If $P' = (1, 2 : 2, 1)$ then τ_3^2 will map P' into $\mathcal{C}$ and not move the other points out of $\mathcal{C}$. Similarly if $P = (1, 2 : 2, 1)$ then τ_3^2 will suffice.

Next suppose that $\alpha(i) \geq 2$ for all i and there exists an i with $\alpha(i) = 2$. Then $2s = 4m - 8 \geq 2m$ gives that $m \geq 4$. Again we suppose $\alpha(1) = 2$, using K^1, if necessary. Let the two points containing 1 be $P = (1, a : b, c)$ and

$Q = (1, u : v, w)$. If $a = u = 1$ then $\sigma_2^1 \in H^1$ will map these to $(1, 2 : b, c)$ and $(1, 2 : v, w)$, and so there are only two main cases to consider, the other one being $P = (1, 1 : a, b)$ and $Q = (1, 2 : u, v)$.

Suppose $P = (1, 2 : 2, 1)$ and $Q = (1, 2 : v, w)$, so $Q \in \mathcal{C}$. Then take $a \neq 1, 2, v$, $a \in \{1 \dots m\}$ (possible because $m \geq 4$), $\tau_a^2 \in K^2$ maps P to $(1, 2 : a, 1)$ and either fixes Q or maps it to $(1, 2 : a, w)$.

If $P = (1, 1 : a, b)$ and $Q = (1, 2 : u, v)$, then we need to map P to $(1, 1 : m, 2)$. Either $\tau_a^m \in K^m$, or $\sigma_b^m \in H^m$, or $\tau_a^m \sigma_b^m$, or ι_g will achieve this; Q can only map to another point of the form $(1, 2 : c, d)$ under these, and should the point be $(1, 2 : 2, 1)$, then τ_3^2 can be used to map it into $\mathcal{C}$, and not move $(1, 1 : m, 2)$ since $m \geq 4$. Thus S will deal with all these cases.

Finally suppose $\alpha(i) \geq 3$ for all i and there exists an i with $\alpha(i) = 3$. Then $2t = 4m - 8 \geq 3m$ gives that $m \geq 8$. Again with K^1 we can ensure that $\alpha(1) = 3$, and using the same argument as in the case of two points, we see that $K^1 H^1$ will reduce the problem to the two cases:
(i) $P = (1, 2 : a, b)$, $Q = (1, 2 : c, d)$, $R = (1, 2 : e, f)$
(ii) $P = (1, 2 : a, b)$, $Q = (1, 2 : c, d)$, $R = (1, 1 : e, f)$

Suppose (i), and suppose $P = (1, 2 : 2, 1)$. Then if $k \neq 1, 2, c, e$ and $k \in \{1 \dots m\}$ (possible because $m \geq 8$), then $\tau_k^2 \in K^2$ will map P to $(1, 2 : k, 1)$ and Q and R will remain in $\mathcal{C}$.

Suppose (ii). Then we need to map R to $(1, 1 : m, 2)$ and this can be achieved as in the case of $\alpha(1) = 2$, with τ_e^m and σ_f^m. This will map P and Q into points of the form $(1, 2 : x, y)$. If one should result in $(1, 2 : 2, 1)$, then τ_3^2 will move this point to $\mathcal{C}$ and not take the other two points out of $\mathcal{C}$.

Thus in all cases $S = K^1 H^1 (K^2 \cup K^m) H^m \{\iota, \tau_3^2\}$ will be a PD-set for the code to correct all $t = 2m - 4$ errors. The size of this set is at most $8m(2m - 1) = 16m^2 - 8m$, since $|(K^2 \cup K^m)| = 2m - 1$, due to ι being in both of the sets. ■

Corollary 2 *For $m, n \geq 3$ and mn even, if C is the binary code of $L_m(n)$, then $K^1 H^1 (K^2 \cup K^m) H^m \{\iota, \tau_3^2\}$ is an s-PD-set for C of size $4m^2n^2 - 2mn^2$ for $s \leq 2m - 1$ using the information set $\mathcal{I}$.*

PROOF. This follows from the proposition and is restricted to the even case since our arguments excluded $(1, 2 : m, n)$ being an information point. The rest goes through, since $\alpha(i) \leq 3$ for some i. ■

Proposition 6 *Let C be the binary code of the graph $L_m(n)$ for $m, n \geq 3$. Then taking for information set $\mathcal{I}$ for mn even, or $\mathcal{I}^*$ for mn odd, the set*

$S = K^1H^1H^2D^m$ is an s-PD-set for C, for $s < 3m/2$, of size mn^3.

In particular, if $n = 3$ and m is odd, then S is a PD-set of size $27m$ for C, a $[\frac{9}{2}m(m-1), 3m-1, 3m-3]_2$ code.

PROOF. From Lemma 3 we see that for $s < 3m/2$ errors, i.e. $\mathcal{T}$ having s points, there is an i for which $\alpha(i) \leq 2$. Again we use K^1 to ensure that $\alpha(1) \leq 2$, and as in Proposition 5, consider the possibilities for $\alpha(1) = 0, 1, 2$.

If $\alpha(1) = 0$ then ι will suffice. Suppose $\alpha(1) = 1$ and let $P = (1, i : a, b) \in \mathcal{T} \cap \mathcal{I}^*$. Then if $i = 1, (a, b) \neq (2, 1)$, use $\sigma_n^1 \in H^1$; if $i \neq 1, (a, b) = (2, 1)$, use $\sigma_n^2 \in H^2$; if $P = (1, 1 : 2, 1)$, use $\sigma_n^1\sigma_n^2 \in H^1H^2$; if $P = (1, 2 : m, n)$, use $\sigma_2^1 \in H^1$. Thus maps in $K^1H^1H^2$ will suffice to map $\mathcal{T}$ into $\mathcal{C}$.

Suppose $\alpha(1) = 2$ and let $P = (1, i : a, b)$ and $Q = (1, j : c, d)$ be in $\mathcal{T}$. First suppose $i = j$; if $i = j = 1$ then $\sigma_n^1 \in H^1$ will map P and Q to points $(1, n : a, b)$ and $(1, n : c, d)$ which are either both in $\mathcal{C}$, or $(a, b) = (2, 1)$, in which case the map $\sigma_e^2 \in H^2$, where $e \neq 1, d$, will map them both into $\mathcal{C}$. Thus $K^1H^1H^2$ suffices so far.

If $i = j \neq 1, 2$, then H^2 will work, as above. If $i = j = 2$, then $P = (1, 2 : a, b)$ and $Q = (1, 2 : c, d)$ and at least one is assumed to be in $\mathcal{I}$. If $P = (1, 2 : 2, 1)$ and $Q \in \mathcal{C}$, then $\sigma_e^2 \in H^2$, where $e \neq 1, d$ will map all the points to $\mathcal{C}$. If $P = (1, 2 : 2, 1)$ and $Q = (1, 2 : m, n)$ (in the mn odd case), then $\sigma_2^2\delta_1^m \in H^2D^m$ will map all into $\mathcal{C}$. If $P = (1, 2 : m, n)$ and $Q = (1, 2 : m, d)$, then use $\delta_e^m \in D^m$, where $e \neq n, d$. Thus $K^1H^1H^2D^m$ suffices.

If $i \neq j$, then if $i = 1$, $\sigma_k^1 \in H^1$, where $k \neq j$, will map the points to $P = (1, k : a, b)$ and $Q = (1, j : c, d)$, where $1 < k < j \leq n$, say. If $(a, b) = (2, 1)$ then σ_e^2, where $e \neq 1, d$, will map the points to $\mathcal{C}$ provided that $Q \neq (1, 2 : m, n)$. If $Q = (1, 2 : m, n)$ then the map δ_e^m, where $e \neq n, b$ can be used.

This covers all cases, i.e. $K^1H^1H^2D^m$ acts as an s-PD-set.

Note that when $n = 3$ and m is odd, we have a $[9m(m-1)/2, 3m-1, 3m-3]_2$ code that can correct up to $t = (3m-5)/2$ errors. Thus $2t < 3m$ so that the s-PD-set is a PD-set. ■

Following from the proof of this proposition, we get

Corollary 3 *For $m, n \geq 3$ and C the binary code of $L_m(n)$, then using the information set $\mathcal{I}$ or $\mathcal{I}^*$,*

- *K^1 is an s-PD-set of size m for C for $s \leq \lceil m/2 \rceil - 1$;*
- *$K^1H^1H^2$ is an s-PD-set of size mn^2 for C for $s \leq m - 1$.*

PROOF. The proof is immediate from the proof of the previous proposition, noting that from the earlier discussion, if $2s \leq m-1$ then $\alpha(i) = 0$ for some i for any set of s points, and if $s \leq m-1$ then $\alpha(i) \leq 1$ for some i. ■

Finally we obtain a condition involving the size of n.

Proposition 7 *Let C be the binary code of $L_m(n)$ where $m, n \geq 3$. Using the information set $\mathcal{I}$ or $\mathcal{I}^*$,*

(1) if $s \leq \lceil n/2 \rceil - 1$, then H_n is an s-PD-set of size n for mn even, and $H_n\{\iota, \delta_1^m\}$ is an s-PD-set of size $2n$ for mn odd;
(2) if $s \leq n-1$ then $H_nH^1H^2$ is an s-PD-set of size n^3 for mn even, and $H_nH^1H^2\{\iota, \delta_1^m\}$ is an s-PD-set of size $2n^3$ for mn odd;
(3) if $m = 3$ and $n \geq 3$ is odd, then $H_nH^1H^2\{\iota, \delta_1^m\}$ is a PD-set of size $2n^3$ for C, a $[3n^2, 3n-1, 2n]_2$ code.

PROOF. Considering now $\beta(j)$ and Lemma 3, for the first condition, $k = 1$, i.e. $s \leq (n-1)/2$. There is a j such that $\beta(j) = 0$ and we can use H_n to map $\mathcal{T}$ to a set of s points for which $\beta(1) = 0$. First take mn even. In this case, since $1 \notin B$, it follows that the set in now in $\mathcal{C}$. Thus H_n will suffice as an s-PD-set.

Now take mn odd, so that $P = (1, 2 : m, n) \in \mathcal{I}$. Using H_n to ensure that $\beta(1) = 0$, if P is in the new s-set, then the map δ_1^m will move all the points into $\mathcal{C}$. This proves the first part of the proposition.

Taking now $k = 2$, if $s \leq n-1$ then we can assume $\beta(1) \leq 1$ using H_n again. If $\beta(1) = 0$, use the same argument as above. Thus now suppose $\beta(1) = 1$. Assuming the set $\mathcal{T}$ is not in $\mathcal{C}$, there is one point of the form $(1, 1 : j, k)$, where $k \neq 1$, or $(1, k : 2, 1)$, where $k \neq 1$, and possibly the point $(1, 2 : m, n)$.

If $(1, 1 : j, k) \in \mathcal{T}$, $((j, k) \neq (m, n)$ since we assume that the point is in $\mathcal{I})$, then we can find an e, $1 \leq e \leq n$, such that $(1, e : j, k) \notin \mathcal{T}$, since there are n such elements and our set has at most $n-1$ elements. The map $\sigma_e^1 \in H^1$ will map $\mathcal{T}$ to a set with $\beta(1) = 0$, and then δ_1^m can be used if necessary.

If $(1, k : 2, 1) \in \mathcal{T}$, then there is an e such that $(1, k : 2, e) \notin \mathcal{T}$, so the map $\sigma_e^2 \in H^2$ can be used, followed by δ_1^m if necessary.

Finally, if $m = 3$ and n is odd, then C corrects at most $t = n-1$ errors, so we have a PD-set. ■

5 Conclusion

Based on computations and similar arguments to those in the propositions, we believe that the codes for all the graphs $L_m(n)$ will have PD-sets for full error correction, although we have only found explicit sets for certain classes.

Acknowledgement

The authors thank the reviewers for their careful reading of the paper and for their useful suggestions.

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] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://magma.maths.usyd.edu.au/magma/.

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

[4] 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.

[5] J. D. Key and J. Limbupasiriporn. Permutation decoding of codes from Paley graphs. *Congr. Numer.*, 170:143–155, 2004.

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

[7] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding of codes from finite geometries. *Finite Fields Appl.*, 12:232–247, 2006.

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

[9] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples and permutation decoding. *Ars Combin.*, 79:11–19, 2006.

[10] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*,To appear.

[11] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.* (Special issue dedicated to J. Seberry), To appear.

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

[13] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1998.

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