Discrete Mathematics 310 (2010) 1884–1897

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Codes from incidence matrices and line graphs of Hamming graphs

W. Fish, J.D. Key*, E. Mwambene

Department of Mathematics and Applied Mathematics, University of the Western Cape, 7535 Bellville, South Africa

ARTICLE INFO

Article history:
Received 14 September 2009
Received in revised form 2 February 2010
Accepted 17 February 2010
Available online 12 March 2010

Keywords:
Hamming graphs
Line graphs
Incidence matrices
Codes

ABSTRACT

We examine the p-ary codes, for any prime p, that can be obtained from incidence matrices and line graphs of the Hamming graphs, $H(n, m)$, obtaining the main parameters of these codes. We show that the codes from the incidence matrices of $H(n, m)$ can be used for full permutation decoding for all $m, n \geq 3$.

1. Introduction

Codes obtained from the row span of an incidence matrix G of a regular graph Γ of some classes of graphs have been seen to share certain properties that can make such classes useful for practical purposes: if $\Gamma = (V, E)$ is a graph of valency ν, and $|V| = N$, then G is an $N \times \frac{1}{2}N\nu$ matrix of 0s and 1s with rows labelled by the vertices, columns by the edges; the code $C_p(G)$ spanned by the rows of G over $\mathbb{F}_p$, for any prime p, might be $\left[\frac{1}{2}N\nu, N, \nu\right]_p$ or $\left[\frac{1}{2}N\nu, N-1, \nu\right]_p$ (if $p = 2$), and every minimum vector a scalar multiple of the incidence vector of the set of edges through a vertex, i.e. a row of G. Furthermore, there is often a gap in the weight enumerator between ν and $2(\nu - 1)$, the latter arising from the difference of two rows; see [6,12,13] for two particular classes. If $L(\Gamma)$ denotes the line graph (see Section 2 for the definition) of Γ, then the code spanned by the rows of an adjacency matrix A of $L(\Gamma)$ over $\mathbb{F}_p$ will be a subcode of $C_2(G)$ if $p = 2$, of minimum weight in the range $[\nu, 2(\nu - 1)]$; if p is odd, the code is less interesting, being of minimum weight at most 4 if Γ has a closed path of length 4. We look here at this question for the Hamming graphs.

The Hamming graph $H(n, m)$, for n, m integers, is the graph with vertices the m^n n-tuples of R^n, where R is a set of size m, and adjacency defined by two n-tuples being adjacent if they differ in one coordinate position. For example, the n-cube Q_n is $H(n, 2)$ with $R = \mathbb{F}_2$. The number of edges of $H(n, m)$ is $\frac{1}{2}m^n(m-1)n$. The codes from incidence matrices and line graphs of $H(n, m)$ thus have length $\frac{1}{2}m^n(m-1)n$.

Our main results are summarized in the following theorem, where, in all cases, if A is a matrix and p a prime, $C_p(A)$ denotes the row span of A over $\mathbb{F}_p$:

Theorem 1. *Let $G_n(m)$ be an $m^n \times \frac{1}{2}m^n(m-1)n$ incidence matrix for the Hamming graph $H(n, m)$. Let $L(H(n, m))$ denote the line graph of $H(n, m)$, $A_n(m)$ a $\frac{1}{2}m^n(m-1)n \times \frac{1}{2}m^n(m-1)n$ adjacency matrix for $L(H(n, m))$, $L_n(m)$ a $\frac{1}{2}m^n(m-1)n \times \frac{1}{2}m^n(m-1)n((m-1)n-1)$ incidence matrix, for $L(H(n, m))$, and $J_n(m)$ a $\frac{1}{2}m^n(m-1)n((m-1)n-1) \times \frac{1}{2}m^n(m-1)n((m-1)n-1)(2(m-1)n-3)$ incidence matrix for $L(L(H(n, m)))$. Then*

[*] Corresponding author.
E-mail address: keyj@ces.clemson.edu (J.D. Key).

0012-365X/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2010.02.010

1. *For $n \geq 1$, $m \geq 3$, $C_2(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n - 1, (m-1)n\right]_2$ and $C_p(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n, (m-1)n\right]_p$ for p odd. For $m = 2$, p any prime, $C_p(G_n(2)) = [2^{n-1}n, 2^n - 1, n]_p$.*
   For $n \geq 2$, all p and $m \geq 3$, and for $n \geq 3$ and $m = 2$, the minimum words are the non-zero scalar multiples of the rows of $G_n(m)$.
   For $n \geq 2$, $C_2(G_n(m))^\perp$ has minimum weight 3 for $m \geq 3$; $C_p(G_n(m))^\perp$ has minimum weight 4 for p odd, any m, and for $p = 2 = m$.
2. *For m odd, $C_2(A_n(m)) = C_2(G_n)$. For m even, $C_2(A_n(m))$ is the subcode of $C_2(G_n)$ spanned by the differences of the rows of G_n.*
   For p odd, $C_p(A_n(m))$ has minimum weight at most 4.
3. *For $n \geq 3$, $C_2(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n - 1, 2(n-1)]_2$ and $C_p(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n, 2(n-1)]_p$ for p odd. The minimum words are the scalar multiples of the rows of $L_n(2)$.*
   For all p, $C_p(L_n(2))^\perp$ has words of weight 4, and for $p = 2$ it has minimum weight 3.
4. *For $n \geq 3$, $C_2(J_n(2)) = [2^{n-1}n(n-1)(2n-3), 2^{n-1}n(n-1) - 1, 2(2n-3)]_2$ and $C_p(J_n(2)) = [2^{n-1}n(n-1)(2n-3), 2^{n-1}n(n-1), 2(2n-3)]_p$ for p odd. For all p the minimum words are the scalar multiples of the rows of $J_n(2)$.*

The automorphism group of these graphs and codes is $S_m \wr S_n$. In its action of degree $\frac{1}{2}m^n(m-1)n$ on the edge set of $H(n, m)$, any transitive subgroup of it can be used for full permutation decoding using the code $C_p(G_n(m))$ and any information set.

A transitive subgroup of $S_m \wr S_n$ of order $m^n(m-1)n$ is described in Section 9.

We have used Magma [2,4] for computations for small values of the parameters in order to get an idea of what general results may hold. The proofs of the various parts of the theorem will follow from propositions in the following sections. We give some background definitions and notation in Sections 2 and 3. The result for permutation decoding is in Section 9. Finally, in Section 10 we discuss briefly these ideas applied to the graphs $H^k(n, m)$ from the Hamming association scheme.

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* $C_F(\mathcal{D})$ 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 $\text{rank}_p(\mathcal{D})$, 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* $\text{wt}(v)$ of a vector v is the number of non-zero coordinate entries. The *support*, $\text{Supp}(v)$, of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\text{Supp}(v)| = \text{wt}(v)$. The *distance* $d(u, v)$ between two vectors u, v is the number of coordinate positions in which they differ, i.e., $\text{wt}(u-v)$. 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. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. 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. If we need to specify the length $\boldsymbol{m}$ of the all-one vector, we write $\boldsymbol{\jmath_m}$. A *constant vector* is one whose only non-zero entries are 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 $\text{Aut}(C)$. Any code is isomorphic to a code with generator matrix in so-called *standard form*, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. 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. If $x, y \in V$ and x and y are adjacent, we write $[\boldsymbol{x}, \boldsymbol{y}]$ for the edge in E that they define. A graph is *regular* if all the vertices have the same valency. An *adjacency matrix* A of a graph with N vertices 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 $\Gamma = (V, E)$ is a $|V| \times |E|$ matrix B with rows labelled by the vertices and columns by the edges and entries $b_{i,j} = 1$ if the vertex labelled by row i is on the edge labelled by column 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 $L(\Gamma)$ 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. 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 $\text{rank}_p(A)$ 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. It is also the code over $\mathbb{F}_p$ of the neighbourhood design. Similarly, if B is an incidence matrix for Γ, $C_p(B)$ denotes the row span of B over $\mathbb{F}_p$ and is the code of the design with blocks the rows of B, in the case that Γ is regular. If M is an adjacency matrix for $L(\Gamma)$ where Γ is regular of valency k, N vertices, e edges, then

$$BB^T = A + kI_N \quad \text{and} \quad B^TB = M + 2I_e. \tag{1}$$

Permutation decoding, first developed by MacWilliams [16], involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [17, Chapter 16, p. 513] and Huffman [5, Section 8]. In [10,15] 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 $s \le t$ 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 [5] and requires that the generator matrix is in standard form. Furthermore, there is a combinatorial lower bound for $|\mathcal{S}|$; see [9,18], or [5].

3. Hamming graphs

The Hamming graph $H(n, m)$, for n, m integers, is the graph with vertices the m^n n-tuples of R^n, where R is a set of size m which we will take to be a ring with identity (in particular $\mathbb{Z}_m$ or $\mathbb{F}_m$ when m is a prime power) and adjacency defined by two n-tuples being adjacent if they differ in one coordinate position. It is a regular graph of valency $(m-1)n$ and $\frac{1}{2}m^n(m-1)n$ edges. Edges will be denoted $[x, x+e]$ where $x, e \in R^n$ and $\mathrm{wt}(e) = 1$. As usual we will denote the standard basis for R^n by $\{e_1, \ldots, e_n\}$, so $e_1 = (1, 0, \ldots, 0)$, for example. It is well known that $\mathrm{Aut}(H(n, m)) = S_m \wr S_n$ (see [3]), where S_n is the symmetric group on the n coordinate positions of R^n, now acting naturally on the n-tuples, and S_m acts on the elements of R. Thus by Whitney [19], $\mathrm{Aut}(L(H(n, m))) = S_m \wr S_n$, where $L(H(n, m))$ is the line graph of $H(n, m)$.

An incidence matrix for $H(n, m)$ will be denoted by $G_n(m)$ and the 1-design defined by taking for points the set $\mathcal{P}_n$ of edges of $H(n, m)$ and for blocks the rows of $G_n(m)$, will be denoted by $\mathcal{G}_n(m)$. Thus if $x \in R^n$, it defines the block $\bar{x}$, where

$$\bar{x} = \{[x, x+e] \mid e \in R^n, \mathrm{wt}(e) = 1\}. \tag{2}$$

Thus $\mathcal{G}_n(m)$ is a 1-$\left(\frac{1}{2}m^n(m-1)n,\ (m-1)n,\ 2\right)$ design.

The following general result about the automorphism groups holds:

Lemma 1. *Let $\Gamma = (V, E)$ be a regular graph with $|V| = N$, $|E| = e$ and valency υ. Let $\mathcal{G}$ be the* 1- $(e, \upsilon, 2)$ *incidence design from an incidence matrix G for Γ. Then* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{G})$.

Proof. Denote the set of points of $\mathcal{G}$ by $\mathcal{P}$ $(=E)$ and the blocks of $\mathcal{G}$ by $\mathcal{B}$. Thus for $P \in V$, $\overline{P}$ is the set of edges through P.

First suppose $\alpha \in \mathrm{Aut}(\Gamma)$. Then α maps edges to edges so it acts naturally on $\mathcal{P}$. Naturally its action on $\mathcal{B}$ is defined so that $(\overline{P})^\alpha = \overline{P^\alpha}$. So if $X \in \overline{P}$, then $X = [P, Q]$, $X^\alpha = [P^\alpha, Q^\alpha]$, so $X^\alpha \in (\overline{P})^\alpha = \overline{P^\alpha}$. So $\alpha \in \mathrm{Aut}(\mathcal{G})$.

Now suppose $\alpha \in \mathrm{Aut}(\mathcal{G})$. Then α acts on $\mathcal{P}$, the edges of Γ, and on the blocks $\mathcal{B}$, so that for $X \in B$, $X^\alpha \in B^\alpha$. We need to define α to act on vertices $P \in V$, and we do this by defining $P^\alpha = Q$ if $(\overline{P})^\alpha = \overline{Q}$. If $[P, Q] \in E$ then we need to show that $[P^\alpha, Q^\alpha] \in E$. Now $[P, Q] \in \overline{P}, \overline{Q}$, so $[P, Q]^\alpha \in (\overline{P})^\alpha, (\overline{Q})^\alpha$. So $[P, Q]^\alpha = [P^\alpha, R] = [Q^\alpha, S]$. Since $P \ne Q$, so that $P^\alpha \ne Q^\alpha$, we must have $[P, Q]^\alpha = [P^\alpha, Q^\alpha]$, so that P^α and Q^α are together on an edge, and hence $\alpha \in \mathrm{Aut}(\Gamma)$. ■

This shows that $\mathrm{Aut}(\mathcal{G}_n(m)) = S_m \wr S_n$. Note that this is in contrast to the automorphism group of the neighbourhood design, which may well be larger; see [7, Proposition 3], where $m = 2$ and the group is larger, and [8, Proposition 3], where $m \ne 2$ and the group is the same as that of the graph.

For $H(n, m)$ we assume a natural ordering on the elements of R. An $m^n \times \frac{1}{2}m^n(m-1)n$ incidence matrix $G_n(m)$ can be written in the following way: take the natural ordering of the rows corresponding to the m-ary representation of the natural numbers from 0 to $m^n - 1$, and divide the rows into m sections R_i, $i = 0, \ldots, m-1$, where the rows in R_i are labelled by the vectors $x = (x_1, \ldots, x_n)$ with $x_n = i$. The columns are ordered so that we first take all the edges between vertices in the rows from R_0, followed by those edges between vertices from rows R_1, up to all those in R_{m-1}. Then take all edges between vertices in rows R_0 and R_1, then R_0 and R_2, up to R_0 and R_{m-1}, then R_2 and R_3, and so on inductively until finally R_{m-2} and R_{m-1}. Thus an incidence matrix $G_n(m)$ will have the following form:

$$G_n(m) = \left[\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c}
G_{n-1}(m) & 0 & 0 & 0 & \cdots & I & I & I & \cdots & 0 & 0 & 0 \\ \hline
0 & G_{n-1}(m) & 0 & 0 & \cdots & I & 0 & 0 & \cdots & 0 & 0 & 0 \\ \hline
0 & 0 & G_{n-1}(m) & 0 & \cdots & 0 & I & 0 & \cdots & 0 & 0 & 0 \\ \hline
0 & 0 & 0 & G_{n-1}(m) & \cdots & 0 & 0 & I & \cdots & 0 & 0 & 0 \\ \hline
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline
0 & 0 & 0 & 0 & G_{n-1}(m) & 0 & 0 & 0 & \cdots & 0 & I & I
\end{array}\right], \tag{3}$$

where $I = I_{m^{n-1}}$ and there are $m-1$ of them in each of the m sets R_i of rows. The columns are also in blocks, and there are $\binom{m+1}{2}$ of them. There are m column blocks C_i for which the only entry is G_{n-1}, and these are the first m column blocks, $C_1, \ldots, C_m$.

For example, for $m = 2$ and 3,

$$G_n(2) = \left[\begin{array}{c|c|c} G_{n-1}(2) & 0 & I \\ \hline 0 & G_{n-1}(2) & I \end{array}\right], \qquad G_n(3) = \left[\begin{array}{c|c|c|c|c|c} G_{n-1}(3) & 0 & 0 & I & I & 0 \\ \hline 0 & G_{n-1}(3) & 0 & I & 0 & I \\ \hline 0 & 0 & G_{n-1}(3) & 0 & I & I \end{array}\right], \tag{4}$$

where $I = I_{2^{n-1}}$ in $G_n(2)$ and $I = I_{3^{n-1}}$ in $G_n(3)$.

A general observation about the codes from incidence matrices is in the following lemma:

Lemma 2. *Let $\Gamma = (V, E)$ be a graph such that $V = V_1 \dot{\cup} V_2$ (disjoint union) and every $x \in V_2$ is on an edge with some $y \in V_1$. Let $\Gamma_1 = (V_1, E_1)$ where E_1 is the set of edges between vertices in V_1. If G is an incidence matrix for Γ, G_1 an incidence matrix for Γ_1, p any prime, then* $\mathrm{rank}_p(G) \geq \mathrm{rank}_p(G_1) + |V_2|$.

Proof. We order the rows and columns of G as follows: for the rows we take V_1 followed by V_2. For the columns we first take all the edges between members of V_1, and then follow with edges between V_1 and V_2, and finally edges between vertices in V_2. Then

$$G = \left[\begin{array}{c|c|c} G_1 & X & 0 \\ \hline 0 & Y & Z \end{array}\right],$$

where Y has only one entry 1 in each column and there are at least $|V_2|$ such columns, so the rank of the second set of rows is at least $|V_2|$, and clearly also at most $|V_2|$. The top set has rank at least that of G_1. ■

The following general result for connected graphs is from [14]:

Result 1. *Let $\Gamma = (V, E)$ be a graph, G an incidence matrix for Γ, $C_p(G)$ the row-span of G over $\mathbb{F}_p$. If Γ is connected then* $\dim(C_2(G)) = |V| - 1$, *and if Γ is connected and has a closed path of odd length ≥ 3, then* $\dim(C_p(G)) = |V|$ *for odd p.*

4. Codes from an incidence matrix for $H(n, m)$

In this section we consider the codes $C_p(G_n(m))$. All the notation will be as defined in Section 3. We take R to be a ring, in fact usually $\mathbb{Z}_m$, or a field if m is a prime power.

We first need a lemma.

Lemma 3. *Let Γ be a graph, G an incidence matrix for Γ, and (P, Q, R, S) a closed path in Γ. For any prime p, if $C = C_p(G)$, then*

$$u = v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,R]} \in C^{\perp}.$$

In particular, for p any prime, $m \geq 2$, then for $n \geq 2$, $C_p(G_n(m))^{\perp}$ contains the weight-4 word

$$u(x, x+e, x+f) = v^{[x,x+e]} - v^{[x,x+f]} - v^{[x+e+f,x+e]} + v^{[x+e+f,x+f]}, \tag{5}$$

where $x \in R^n$, $\mathrm{wt}(e) = \mathrm{wt}(f) = 1$, *$e \neq f$. Further, $C_p(G_n(m))^{\perp}$ has minimum weight 4 for p odd, any m, and for $p = 2 = m$; $C_2(G_n(m))^{\perp}$ has minimum weight 3 for $m \geq 3$.*

Proof. For the first statement, note that it is clear that $(u, r) = 0$ for any row r of G. Then note that $(x, x+e, x+e+f, x+f)$ is a closed path in $H(n, m)$ for $n \geq 2$. It is easy to verify that $C^{\perp}$ cannot contain vectors of weight 2. Vectors of weight 3 can only occur in the case $p = 2$, $m > 2$ and will have the form $v^{[x,x+\alpha e]} + v^{[x,x+\beta e]} + v^{[x+\alpha e,x+\beta e]}$, where $\mathrm{wt}(e) = 1$, $\alpha, \beta \in R$, and $\alpha \neq \beta$. ■

We prove our results for $m = 2$ separately as these have already been studied for $p = 2$ (see [6]), and we can use a different proof in this case.

Proposition 1. *Let $G_n(2)$ be a $2^n \times 2^{n-1}n$ incidence matrix for $H(n, 2)$.*

For $n \geq 1$, p any prime, $C_p(G_n(2)) = [2^{n-1}n, 2^n - 1, n]_p$. For $n \geq 3$ the minimum words are the scalar multiples of the rows of G_n and $C_p(G_n(2))^{\perp}$ is spanned by the weight-4 vectors of Eq. (5).

For $n \geq 3$, $\mathrm{Aut}(C_p(G_n(2))) = S_2 \wr S_n = T_n \rtimes S_n$, *where T_n is the translation group on $\mathbb{F}_2^n$.*

Proof. For the dimension, it is clearly true for $n = 1$. Assume it is true for $n - 1$, where $n \geq 2$. Then it easily follows from Eq. (4) that the rank of G_n is $2^n - 1$, by induction.

Write $C = C_p(G_n(2))$. To prove the statement concerning the minimum weight, we show that the weight of a word in the dual to $C^{\perp}$ must be at least n by examining combinatorial properties of the supports of the weight-4 vectors. Let $\mathcal{B}_n$ be the set of supports of the vectors $u(a, b, c)$ as defined in Eq. (5). Then $(\mathcal{P}_n, \mathcal{B}_n)$ is a 1-$(2^{n-1}n, 4, r)$ design, where $r = (n-1)$, since the blocks containing $[x, x + e_i]$ are $u(x, x + e_i, x + e_j)$ where $i \neq j$. Furthermore, any two points are together on one or no blocks, since two points determine the block.

Let $w \in C$ and $\mathrm{Supp}(w) = \mathcal{S}$, where $|\mathcal{S}| = s$. Let $P = [0, e_1] \in \mathcal{S}$. Suppose that in $\mathcal{S}$ there are k points of the type that are on a block with P, and ℓ that are not. 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 $z_2 + 2z_3 + 3z_4 = k = s - 1 - \ell$. Thus $r = n - 1 \leq z_2 + 2z_3 + 3z_4 \leq (s - 1)$ so $s \geq n$. Since there are vectors of weight n, this is the minimum weight. Suppose $s = n$. Thus the inequalities above are equalities and so $z_3 = z_4 = 0$, and $\ell = 0$. Thus $\mathcal{S}$ consists of $[0, e_1]$ and points of the form $[0, e_j]$, $[e_1, e_1 + e_j]$, $[e_j, e_1 + e_j]$, and each block of $\mathcal{B}_n$ meets $\mathcal{S}$ exactly twice, since this argument applies to any point of $\mathcal{S}$. Furthermore, since $\ell = 0$ for each point of $\mathcal{S}$, any two points of $\mathcal{S}$ are on a block. This implies that $\mathcal{S} = \bar{0}$ or $\bar{e_1}$, and since n is the minimum weight, $w = \alpha\bar{0}$ or $\alpha\bar{e_1}$.

That the vectors of weight 4 span $C^{\perp}$ follows in the same way as for the binary codes, as proved in [6, Proposition 15], by finding $\dim(C^{\perp})$ linearly independent weight-4 vectors of this form.

For the statement regarding the automorphism group of $C_p(G_n(2))$, we know that for $n \geq 3$ the words of weight n are the scalar multiples of the rows of $G_n(2)$, i.e. of the incidence vectors of the blocks of $\mathcal{G}_n(2)$, and since any automorphism of the code must preserve weight classes, we see that the blocks of the design are preserved, and thus we have an automorphism of the design. Now use Lemma 1. ∎

Note. The group $S_2 \wr S_n = T \rtimes S_n$ is known as the generalized symmetric group.

Now we take $m \geq 3$. Notice that $H(1, m) = K_m$, where K_m is the complete graph on m vertices, and thus $G_1(m)$ is an $m \times \binom{m}{2}$ incidence matrix for K_m. This matrix is written as M_m in [12] where it is proved that, writing

$$G_1(m) = M_m = \begin{bmatrix} M_{m-1} & I_{m-1} \\ 0 \cdots 0 & 1 \cdots 1 \end{bmatrix}, \tag{6}$$

for $m \geq 3$, where $M_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, then $\dim(C_p(M_m)) = m$ for $m \geq 3$ and p an odd prime, and that for $m \geq 4$ the minimum weight of $C_p(M_m)$ is $m - 1$ for $m \geq 4$. It is well known that $\dim(C_2(M_m)) = m - 1$, the minimum weight of $C_2(M_m)$ is $m - 1$, and the words of weight $m - 1$ are the rows of M_m. We need these facts in the proposition below, where we exclude the case $m = 2$ since this has been examined in Proposition 1 and elsewhere (see [6]).

Proposition 2. *Let $G_n(m)$ be an $m^n \times \frac{1}{2}m^n(m-1)n$ incidence matrix for $H(n, m)$.*
For $n \geq 2$, p odd, $m \geq 3$,

- $C_p(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n, (m-1)n\right]_p$;
- $C_2(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n - 1, (m-1)n\right]_2$.

For all p, the minimum vectors are the non-zero scalar multiples of the rows of $G_n(m)$. For $n \geq 2$, $\mathrm{Aut}(C_p(G_n(m))) = S_m \wr S_n$.

Proof. Recall that $\Gamma = H(n, m)$ has m^n vertices, valency $(m-1)n$ and $\frac{1}{2}m^n(m-1)n$ edges. We take $G_n(m)$ as written in Eq. (3).

The statement about the dimension of the codes is clear since $H(n, m)$ is clearly connected so we can use Result 1 immediately for $p = 2$, and also for p odd since $(0, e_1, ae_1)$ for $a \neq 0, 1$ is a closed path of length 3.

Each $w \in C_p(G_n(m))$ is written as a concatenation of vectors w_i, for $1 \leq i \leq \binom{m+1}{2}$, where w_i has length $\frac{1}{2}m^{n-1}(m-1)(n-1)$ if $1 \leq i \leq m$ and length m^{n-1} for $i > m$.

Case (i): *p odd*

For p odd, we need to look first at $m = 3$, since $C_p(G_1(3))$ is the full space $\mathbb{F}_3^3$, of minimum weight 1. So we consider $G_2(3)$ in order to establish an induction base.

$$G_2(3) = \left[\begin{array}{c|c|c|c|c|c} G_1(3) & 0 & 0 & I & I & 0 \\ \hline 0 & G_1(3) & 0 & I & 0 & I \\ \hline 0 & 0 & G_1(3) & 0 & I & I \end{array}\right], \quad \text{where } G_1(3) = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \ I = I_3. \tag{7}$$

First observe that the sum of any two multiples of rows of $G_1(3)$ has weight at least 2, i.e. three rows are needed to get weight 1 from $G_1(3)$. We will show that the minimum weight of $C_p(G_2(3))$ is $(m-1)n = 4$ and that the minimum words are the scalar multiples of the rows of $G_2(3)$.

As mentioned before, we label the column blocks as C_i for $i = 1, \ldots, 6$. We write $w \in C_p(G_2(3))$ as $w = (w_1, w_2, w_3, w_4, w_5, w_6)$ where w_i is that part of w in the column block C_i. If two or three rows from R_0 are taken then we get a vector of weight at least 6, and similarly for R_1, R_2. Similarly if at least one row from each of R_0 and R_1 are taken, and similarly for the other pairs. Now take w a sum of some rows from each of R_0, R_1, R_2. Let r_i, $i = 1, 2, 3$ denote the rows of $G_1(3)$, and ρ_i for $i = 1, \ldots, 9$ the rows of $G_2(3)$. If $w = \sum_{i=1}^{3} \alpha_i\rho_i + \sum_{i=1}^{3} \beta_i\rho_{i+3} + \sum_{i=1}^{3} \gamma_i\rho_{i+6}$ then $w_1 = \sum_{i=1}^{3} \alpha_i r_i$, $w_2 = \sum_{i=1}^{3} \beta_i r_i$, $w_3 = \sum_{i=1}^{3} \gamma_i r_i$, $w_4 = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3)$, $w_5 = (\alpha_1 + \gamma_1, \alpha_2 + \gamma_2, \alpha_3 + \gamma_3)$, $w_6 = (\beta_1 + \gamma_1, \beta_2 + \gamma_2, \beta_3 + \gamma_3)$. Clearly $\mathrm{wt}(w_i) \geq 1$ for $i = 1, 2, 3$ (since the rows of $G_1(3)$ are linearly independent); if $\mathrm{wt}(w_4) < 3$ then $\alpha_1 = -\beta_1$, say, and $\beta_1 + \gamma_1$ and $\alpha_1 + \gamma_1 (= -\beta_1 + \gamma_1)$ are not both zero unless $\alpha_1 = \beta_1 = \gamma_1 = 0$ in which case $\mathrm{wt}(w_i) \geq 2$ for $i = 1, 2, 3$

and so $\mathrm{wt}(w) \geq 6$. So we have $\mathrm{wt}(w) \geq 4$. If we have equality then, since either w_5 or w_6 is not zero, we have $w_4 = 0$ and the same argument will yield that $\alpha_2 = \beta_2 = \gamma_2 = 0$, giving a contradiction. Thus we have the result for $m = 3$ and $n = 2$.

We can now turn to the general value of $m \geq 3$, p odd. To establish the induction base, we know that for $m \geq 4$ the minimum weight of $G_1(m)$ is $m-1$. So we can start our induction at $n = 2$ for $m = 3$ and at $n = 1$ for $m \geq 4$. Suppose the assertion is true for $n-1$. For the minimum weight, we have $w = (w_1, \ldots, w_N) \in C_p(G_n(m))$ where $N = \binom{m+1}{2}$. We consider combinations of rows from R_i for $i = 0, \ldots, m-1$. If w is a sum of $k \geq 2$ rows from R_0 then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + k(m-1) \geq (m-1)(n-1) + k(m-1) = (m-1)n + (m-1)(k-1) > (m-1)n$. Similarly for all the R_i, $i = 1, \ldots, m-1$. If w is a combination of rows from at least two blocks R_i then the components from the $G_{n-1}(m)$ will provide weight at least $2(m-1)(n-1) > (m-1)n$ unless $n = 2$ and so $m \geq 4$ and we are taking just two blocks of rows, so that $\mathrm{wt}(w) \geq 2(m-1)(n-1) + 2(m-2)$, since the blocks containing $I_{m^{n-1}}$ overlap in only one column block. Thus $\mathrm{wt}(w) > (m-1)n$ in this case too. This completes the proof for p odd.

Case (ii): $p = 2$

For $p = 2$, note that any $m^n - 1$ rows of $G_n(m)$ are linearly independent. We can proceed directly by induction, supposing the assertion is true for $n = 1$, from known results concerning M_m. Suppose it is true for $n-1$, where $n-1 \geq 1$. A sum of rows from R_0 will yield zero from the component in $G_{n-1}(m)$ only if all the rows are taken in the sum, in which case the weight is at least $(m-1)m^{n-1} > (m-1)n$ since $m^{n-1} \geq 3^{n-1} > n$ for $n \geq 2$. If w is a combination of rows from at least two blocks R_i and if at least two of the components from $G_{n-1}(m)$ are non-zero then we argue as we did in the case of p odd. So the only case that needs consideration is that case when all the components, or all but one, from the $G_{n-1}(m)$ are zero. If w is a sum of all the rows in k blocks of rows $R_{i_j}, j = 1, \ldots, k$, where $m > k \geq 2$, then $\mathrm{wt}(w) = k(m-1)m^{n-1} > (m-1)n$. Similarly if we take fewer than all the rows from one block R_i, but all the rows in some other blocks R_j. In all events, $\mathrm{wt}(w) > (m-1)n$ if more than one row is taken. This completes the proof for $p = 2$.

The statement regarding the automorphism group of $C_p(G_n(m))$ follows as in Proposition 1. ■

5. Line graphs

We make a few general observations about line graphs and their associated codes.

Let $\Gamma = (V, E)$ be a regular graph with vertex set V, edge set E, and $N = |V|$, $|E| = e$, valency v. $L(\Gamma)$ denotes the line graph of Γ. Then $e = \frac{1}{2}Nv$. We write $L_1 = L(\Gamma)$, and recursively $L_i = L(L_{i-1})$ for $i \geq 2$, and we can write $L_0 = \Gamma$. Let $L_i = (V_i, E_i)$ and write v_i for the valency of L_i. Then by definition $|V_i| = |E_{i-1}|$ and $v_i = 2(v_{i-1} - 1)$ for $i \geq 1$, where $V_0 = V$, $E_0 = E$ and $v_0 = v$. It follows that, for $m \geq 1$,

$$|V_m| = e\prod_{i=0}^{m-2}(2^i v - 2^{i+1} + 1), \qquad |E_m| = e\prod_{i=0}^{m-1}(2^i v - 2^{i+1} + 1), \qquad v_m = 2(2^{m-1}v - 2^m + 1). \tag{8}$$

Example 1. Let $\Gamma = H(n, 2) = Q_n$. Then $N = 2^n$, $v = n$, $e = 2^{n-1}n$. Thus for $m \geq 1$,

$$|V_m| = 2^{n-1}n\prod_{i=0}^{m-2}(2^i n - 2^{i+1} + 1), \qquad |E_m| = 2^{n-1}n\prod_{i=0}^{m-1}(2^i n - 2^{i+1} + 1), \qquad v_m = 2(2^{m-1}n - 2^m + 1). \tag{9}$$

For the Hamming graphs in general, $L(H(n, m))$ has $\frac{1}{2}m^n(m-1)n$ vertices, valency $2((m-1)n-1)$ and $\frac{1}{2}m^n(m-1)n((m-1)n-1)$ edges.

We will denote the neighbourhood design of $L(H(n, m))$ by $\mathcal{L}_n$, where the block defined by the point $[x, x+e]$ is denoted by $\overline{[x, x+e]}$ and given by

$$\overline{[x, x+e]} = \{[x, x+f] \mid \mathrm{wt}(f) = 1, f \neq e\} \cup \{[x+e, x+e+f] \mid \mathrm{wt}(f) = 1, f \neq e\}. \tag{10}$$

The design $\mathcal{L}_n$ is a symmetric 1-$\left(\frac{1}{2}m^n(m-1)n, 2((m-1)n-1), 2((m-1)n-1)\right)$ design.

Below we note some general observations about the codes from line graphs. From the observation that if $(P_1, P_2, \ldots, P_r)$ is a closed path in Γ, where $r \geq 3$, then $([P_1, P_2], [P_2, P_3], \ldots, [P_r, P_1])$ is a closed path in $L(\Gamma)$, so we have immediately from Lemma 3, if (P, Q, R, S) is a closed path in Γ, G_1 an incidence matrix for $L(\Gamma)$, p any prime, then

$$v^{[[P,Q],[P,S]]} + v^{[[Q,R],[R,S]]} - v^{[[P,S],[R,S]]} - v^{[[P,Q],[Q,R]]} \in C_p(G_1)^{\perp}.$$

From this follows:

Lemma 4. *If Γ is a graph with closed paths of length 4, and C is the p-ary code from an incidence matrix for Γ, p any prime, then $C^{\perp}$ has minimum weight at most 4. Furthermore, if G_i is an incidence matrix for $L_i(\Gamma)$, then $C(G_i)^{\perp}$ has minimum weight at most 4, for any $i \geq 1$.*

Also from Lemma 3, if $\Gamma = (V, E)$, $P \in V$, and $\{Q, R, S, T\}$ neighbours of P, then if p is any prime and G_1 is an incidence matrix for $L(\Gamma)$, it follows that

$$v^{[[P,Q],[P,R]]} + v^{[[P,S],[P,T]]} - v^{[[P,Q],[P,T]]} - v^{[[P,R],[P,S]]} \in C_p(G_1)^{\perp}.$$

Recall that if $[P, Q]$ is an edge in Γ then the block of the symmetric design from the neighbours of each point of the line graph $L(\Gamma)$ is denoted by

$$\overline{[P, Q]} = \{[P, R] \mid R \neq Q\} \cup \{[R, Q] \mid R \neq P\}.$$

Proposition 3. *Let Γ be a graph and (P, Q, R, S) a closed path in Γ, p an odd prime. Then*

$$v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,R]} \in C_p(L(\Gamma)).$$

Proof. It can be verified directly that

$$v^{\overline{[P,Q]}} + v^{\overline{[R,S]}} - v^{\overline{[P,S]}} - v^{\overline{[Q,R]}} = -2(v^{[P,Q]} + v^{[R,S]} - v^{[P,S]} - v^{[Q,R]}),$$

and this is not 0 since p is odd. ∎

6. Codes from an adjacency matrix for $L(H(n, m))$

In this section we look at $C_p(L(H(n, m)))$, i.e. codes from an adjacency matrix for the line graph of $H(n, m)$. We can use our results from Section 4 to study these codes. Here $G_n = G_n(m)$ will be a $m^n \times \frac{1}{2}m^n(m-1)n$ incidence matrix for $H(n, m)$ given in the form of Eq. (3), and $A_n = A_n(m)$ will be the corresponding $\frac{1}{2}m^n(m-1)n \times \frac{1}{2}m^n(m-1)n$ adjacency matrix for $L(H(n, m))$. As usual

$$G_n^T G_n = A_n + 2I_{\frac{1}{2}m^n(m-1)n}.$$

Further, we write $G_n = [\mathfrak{G}_{n-1} | \mathfrak{I}_{n-1}]$, as in Eq. (3), where $\mathfrak{G}_{n-1}$ is $m^n \times \frac{1}{2}m^n(m-1)(n-1)$ and $\mathfrak{I}_{n-1}$ is $m^n \times \frac{1}{2}m^n(m-1)$ and

$$\mathfrak{G}_{n-1} = \left[\begin{array}{c|c|c|c|c|c} G_{n-1} & 0 & 0 & 0 & \cdots & \cdots \\ \hline 0 & G_{n-1} & 0 & 0 & \cdots & \cdots \\ \hline 0 & 0 & G_{n-1} & 0 & \cdots & \cdots \\ \hline 0 & 0 & 0 & G_{n-1} & \cdots & \\ \hline \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \hline 0 & 0 & 0 & 0 & \cdots & G_{n-1} \end{array}\right], \qquad \mathfrak{I}_{n-1} = \left[\begin{array}{c|c|c|c|c|c|c} I & I & I & \cdots & 0 & 0 & 0 \\ \hline I & 0 & 0 & \cdots & 0 & 0 & 0 \\ \hline 0 & I & 0 & \cdots & 0 & 0 & 0 \\ \hline 0 & 0 & I & \cdots & 0 & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \cdots & 0 & I & I \end{array}\right],$$

where $I = I_{m^{n-1}}$. There are m blocks of rows and m blocks of columns in $\mathfrak{G}_{n-1}$, $m-1$ copies of I in each block of rows of $\mathfrak{I}_{n-1}$, which has m blocks of rows and $\binom{m}{2}$ blocks of columns.

We will also write

$$\mathfrak{A}_{n-1} = \left[\begin{array}{c|c|c|c|c|c} A_{n-1} & 0 & 0 & 0 & \cdots & \cdots \\ \hline 0 & A_{n-1} & 0 & 0 & \cdots & \cdots \\ \hline 0 & 0 & A_{n-1} & 0 & \cdots & \cdots \\ \hline 0 & 0 & 0 & A_{n-1} & \cdots & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \hline 0 & 0 & 0 & 0 & \cdots & A_{n-1} \end{array}\right],$$

a symmetric $\frac{1}{2}m^n(m-1)(n-1) \times \frac{1}{2}m^n(m-1)(n-1)$ matrix, partitioned into m blocks of rows and columns. Then it is easy to verify that, for $n \geq 2$ and all m, with notation as above,

$$A_n = \left[\begin{array}{c|c} \mathfrak{A}_{n-1} & \mathfrak{G}_{n-1}^T \mathfrak{I}_{n-1} \\ \hline \mathfrak{I}_{n-1}^T \mathfrak{G}_{n-1} & \mathfrak{I}_{n-1}^T \mathfrak{I}_{n-1} \end{array}\right], \tag{11}$$

where $\mathfrak{I}_{n-1}^T \mathfrak{I}_{n-1}$ is a symmetric $m^{n-1}\binom{m}{2} \times m^{n-1}\binom{m}{2}$ matrix with $2(m-2)$ entries 1 in every row and column.

Proposition 4. *For $n \geq 2$, any $m \geq 2$, let $G_n(m)$ be an incidence matrix for $H(n, m)$, $A_n(m)$ an adjacency matrix for the line graph $L(H(n, m))$.*

For m odd, $C_2(A_n(m)) = C_2(G_n(m))$. For m even, $C_2(A_n(m))$ is the subcode of $C_2(G_n(m))$ spanned by the differences of the rows of $G_n(m)$.

For p an odd prime, $C_p(A_n(m))$ has minimum weight at most 4, and for $n \geq 3$ and $m = 2$, $C_p(A_n(2)) \supseteq C_p(G_n(2))^{\perp}$.

Proof. We write $G = G_n(m)$, $A = A_n(m)$. Over $\mathbb{F}_2$ we have $G^T G = A$. Thus $C_2(A) \subseteq C_2(G)$. By Proposition 2 $C_2(G)$ has rank $m^n - 1$. If $\boldsymbol{\jmath} = \boldsymbol{\jmath}_{m^n}$ is the all-one vector of length m^n then $\boldsymbol{\jmath} G = 0$.

Let V be the row span of G^T over $\mathbb{F}_2$ and $C = C_2(A)$. Then $\dim V = m^n - 1$. The map $\tau : V \to C$ is defined by $\tau : v = (v_1, \ldots, v_{m^n}) \mapsto (v_1, \ldots, v_{m^n})G$, so that $V\tau = C$ and $\dim C + \dim \ker(\tau) = \dim V = m^n - 1$. A vector v is in the kernel if and only if $v \in V$ and $vG = \mathbf{0}$, and since $\boldsymbol{\jmath} G = \mathbf{0}$, we need determine when $\boldsymbol{\jmath} \in V$.

Since G^T is spanned by vectors of weight 2, it is an even-weight binary code. If m is odd then m^n is odd and hence $\boldsymbol{\jmath}_{m^n} \notin V$ and thus $\dim C = m^n - 1$ and $C = C_2(G)$. If m is even then $m-1$ is odd and if all the rows of $\mathfrak{I}_{n-1}^T$ are added, we get $\boldsymbol{\jmath}_{m^n} \in V$. Hence $\dim(C) = m^n - 2$. Since this is the same of the dimension of the code spanned by the differences of the rows of G, we have the result.

In the case of $C_p(A_n(m))$ for p odd, Proposition 3 can be applied since $H(n,m)$ clearly has closed paths of length 4. If $m = 2$ then since $C_p(A_n(2))$ contains all the weight-4 vectors of the form described in Eq. (5), by Proposition 1, $C_p(A_n(2)) \supseteq C_p(G_n(2))^{\perp}$. ■

7. Codes from an incidence matrix for $L(H(n, 2))$

We now consider the row span over $\mathbb{F}_p$, for any prime p, of an incidence matrix $L_n(2)$ for the line graph $L(H(n,2))$ of $H(n,2)$ for $n \geq 1$.

We consider a $2^{n-1}n \times 2^{n-1}n(n-1)$ incidence matrix $L_n(2)$ of $L(H(n,2))$ with a particular ordering on the rows and columns. Each row of $L_n(2)$ has $2(n-1)$ entries equal to 1, including the case $n = 1$ in which case the line graph has no edges.

Let $G_n = G_n(2)$ as given in Eq. (4), with rows and columns ordered as described in Section 3. Now for the rows of $L_n(2)$ we use the same ordering we had for the columns of $G_n(2)$. We call these sets R_1, R_2, R_3. For the columns, we assume we have an ordering for $L_{n-1}(2)$, and for the first set of columns for $L_n(2)$ we insert $L_{n-1}(2)$ in the rows R_1. For the next set of columns, we insert $L_{n-1}(2)$ in R_2 to show the edges $[x+e_n, y+e_n]$, $[x+e_n, z+e_n]$, where $[x,y]$, $[x,z]$ is an edge in $L(H(n,2))$. For the next columns we take all edges between those points in R_1 and R_3, followed by those in R_2 and R_3. We need to start with $L_2(2)$, and from our ordering for $G_2(2)$ we can order the columns so that $L_2(2)$ is as follows:

$$G_2(2) = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad L_2(2) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}. \tag{12}$$

Thus, representing 0 by the empty space for clarity,

$$L_3(2) = \left[\begin{array}{cccc|cccc|cccccccc|cccccccc}
1 & 1 & & & & & & & 1 & 1 & & & & & & & & & & & & & & \\
& & 1 & 1 & & & & & & & 1 & 1 & & & & & & & & & & & & \\
1 & & 1 & & & & & & & & & & 1 & 1 & & & & & & & & & & \\
& 1 & & 1 & & & & & & & & & & & 1 & 1 & & & & & & & & \\
\hline
& & & & 1 & 1 & & & & & & & & & & & 1 & 1 & & & & & & \\
& & & & & & 1 & 1 & & & & & & & & & & & 1 & 1 & & & & \\
& & & & 1 & & 1 & & & & & & & & & & & & & & 1 & 1 & & \\
& & & & & 1 & & 1 & & & & & & & & & & & & & & & 1 & 1 \\
\hline
& & & & & & & & 1 & & & & 1 & & & & 1 & & & & 1 & & & \\
& & & & & & & & & 1 & & & & & 1 & & & 1 & & & & & 1 & \\
& & & & & & & & & & 1 & & & 1 & & & & & 1 & & & 1 & & \\
& & & & & & & & & & & 1 & & & & 1 & & & & 1 & & & & 1
\end{array}\right]. \tag{13}$$

In general, for $n \geq 2$, recalling that for $n = 2$ the matrix $L_{n-1}(2)$ has no columns,

$$L_n(2) = \left[\begin{array}{c|c|c|c} L_{n-1}(2) & 0 & X & 0 \\ \hline 0 & L_{n-1}(2) & 0 & W \\ \hline 0 & 0 & Y & Z \end{array}\right], \tag{14}$$

where X, W are $2^{n-2}(n-1) \times 2^{n-1}(n-1)$ matrices, and Y, Z are $2^{n-1} \times 2^{n-1}(n-1)$ matrices. Further, every column of X, Y, Z, W has exactly one non-zero entry 1 in it, and every row of X and W has precisely two non-zero entries 1 in it, while every row of Y and Z has precisely $n-1$ non-zero entries 1 in it. Clearly every row of $L_{n-1}(2)$ has $2(n-2)$ entries equal to 1. We label the column blocks C_i for $i = 1, 2, 3, 4$.

We first need a lemma that will be used as our induction base. The notation is as given above.

Lemma 5. *$C_2(L_3(2)) = [24, 11, 4]_2$ and for p odd $C_p(L_3(2)) = [24, 12, 4]_p$. The vectors of weight 4 are the scalar multiples of the rows of $L_3(2)$ for all p.*

Proof. For $p = 2$ we can simply use Magma to verify this for the binary code. Thus take p odd. It is easy to see that $C_p(L_2(2))$ has dimension 3 and minimum weight 2. However, not all the weight-2 vectors are scalar multiples of the rows. Further, writing the rows of $L_2(2)$ as r_i for $1 \leq i \leq 4$, any three of the rows are linearly independent, and $w = \sum_{i=1}^{4} \alpha_i r_i = (\alpha_1 + \alpha_3, \alpha_1 + \alpha_4, \alpha_2 + \alpha_3, \alpha_2 + \alpha_4) = 0$ only if $\alpha_1 = \alpha_2 = -\alpha_3 = -\alpha_4$.

Using Eq. (13), we label the submatrix of the first four rows of $L_3(2)$ as R_1, the next four as R_2 and the last four as R_3. Let $C = C_p(L_3(2))$. Then any vector $w \in C$ can be viewed as a concatenation of vectors in the four partitions of the columns. So we write $w = (w_1, w_2, w_3, w_4)$ where w_1 and w_2 are in $\mathbb{F}_p^4$ and w_3 and w_4 are in $\mathbb{F}_p^8$. Thus $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4)$.

To show that C has dimension 12, notice that $([0, e_1], [e_1, e_1+e_2], [e_1+e_2, e_1+e_2+e_3], [e_1+e_2+e_3, e_1+e_3], [e_1+e_3, e_1])$ is a closed path of odd length 5, so we can use Result 1 since the graph is clearly connected.

To prove the statement about the minimum weight and words we take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 2k$. If $w_1 = 0$ then from the above discussion we must have $k = 4$ and thus $\mathrm{wt}(w) = 8$. If $w_1 \neq 0$ then $\mathrm{wt}(w) \geq 2 + 2k \geq 4$, with equality only when $k = 1$ and we have a multiple of a row. The same argument applies to a sum of rows from R_2, since W is equivalent to X. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = 4k \geq 4$ with equality only if $k = 1$.

If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_2, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 2k + 2m \geq 2(k + m) \geq 4$ with equality only if $k = m = 1$ and $w_1 = w_2 = 0$, and this cannot happen. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 2m$. If $w_1 = 0$ then $k = 4$ and $\mathrm{wt}(w) = \mathrm{wt}(w_3) + 2m > 4$ if $m \geq 3$. If $m = 1$ then $\mathrm{wt}(w_3) \geq 6$ since $w_3 = \alpha(1, 1, 1, 1, -1, -1, -1, -1) + \beta y$ where y is a row of Y and has weight 2. If $m = 2$ then $w_3 \neq 0$ so all words we get are of weight greater than 4. So $\mathrm{wt}(w_1) \geq 2$, and so $\mathrm{wt}(w) \geq 4$ with equality only if $m = 1$, $\mathrm{wt}(w_1) = 2$ and $w_3 = 0$. The latter is impossible since the rows of X with one row of Y are linearly independent, where X and Y are as shown in Eq. (13). A similar argument applies to w a sum of rows from R_2 and R_3. Thus we cannot get vectors of weight 4 this way.

Finally we take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $j \geq 1$ non-zero scalar multiples of rows from R_2 and $m \geq 1$ non-zero scalar multiples of rows from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4)$. Denoting the 12 rows of L_3 by r_i for $1 \leq i \leq 12$, write $w = \sum_{i=1}^{4} \alpha_i r_i + \sum_{i=1}^{4} \beta_i r_{4+i} + \sum_{i=1}^{4} \gamma_i r_{8+i}$ where k of the α_i, m of the β_i and j of the γ_i are not zero. From Eq. (13) we see that

$$w_3 = (\alpha_1 + \gamma_1, \alpha_1 + \gamma_2, \alpha_2 + \gamma_3, \alpha_2 + \gamma_4, \alpha_3 + \gamma_1, \alpha_3 + \gamma_3, \alpha_4 + \gamma_2, \alpha_4 + \gamma_4). \tag{15}$$

If $w_3 = 0$ then $\alpha_i = \alpha = -\gamma_i$ for all $1 \leq i \leq 4$, and hence $k = m = 4$, and $\mathrm{wt}(w_1) = 4$. It also follows from Eq. (15) that if $w_3 \neq 0$ then $\mathrm{wt}(w_3) \geq 2$. The same argument applies to w_4, so if $w_4 = 0$ then $m = j = 4$, and $\mathrm{wt}(w_2) = 4$, so $\mathrm{wt}(w) > 4$. So $w_4 \neq 0$ and hence $\mathrm{wt}(w_3) \geq 2$ and $\mathrm{wt}(w) \geq 6$. So we can assume neither $w_3, w_4 \neq 0$. Then $\mathrm{wt}(w) \geq 6$ if one of w_1 or w_2 is not 0. So supposing $w_1, w_2 = 0$ then $k = 4 = j$, and, with $\alpha, \beta \neq 0$,

$$\begin{aligned} w_3 &= \alpha(1, 1, 1, 1, -1, -1, -1, -1) + (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_1, \gamma_3, \gamma_2, \gamma_4) \\ &= (\alpha + \gamma_1, \alpha + \gamma_2, \alpha + \gamma_3, \alpha + \gamma_4, -\alpha + \gamma_1, -\alpha + \gamma_3, -\alpha + \gamma_2, -\alpha + \gamma_4). \end{aligned}$$

From this we see that $\mathrm{wt}(w_3) \geq 4$. Similarly,

$$\begin{aligned} w_4 &= \beta(1, 1, 1, 1, -1, -1, -1, -1) + (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_1, \gamma_3, \gamma_2, \gamma_4) \\ &= (\beta + \gamma_1, \beta + \gamma_2, \beta + \gamma_3, \beta + \gamma_4, -\beta + \gamma_1, -\beta + \gamma_3, -\beta + \gamma_2, -\beta + \gamma_4). \end{aligned}$$

So $\mathrm{wt}(w_4) \geq 4$, and we cannot get a vector of weight at most 4 in this way. This completes the proof. ■

Proposition 5. *For $n \geq 1$, let $L_n(2)$ be a $2^{n-1}n \times 2^{n-1}n(n-1)$ incidence matrix for $L(H(n, 2))$.*

For $n \geq 3$,

- *$C_2(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n - 1, 2(n-1)]_2$;*
- *$C_p(L_n(2)) = [2^{n-1}n(n-1), 2^{n-1}n, 2(n-1)]_p$ for p odd.*

For all p, the minimum words are the scalar multiples of the rows of $L_n(2)$.

For all p, $n \geq 2$, $C_p(L_n(2))^{\perp}$ has minimum weight at most 4, and for $p = 2$, $n \geq 3$, it has minimum weight 3. For $n \geq 3$, $\mathrm{Aut}(C_p(L_n(2))) = S_2 \wr S_n$.

Proof. *Case* (i): *p odd*

We prove the result stated by induction, having established it in Lemma 5 for $n = 3$.

Suppose the statement is true for $n - 1$, where $n \geq 4$, and consider $L_n(2)$ as shown in Eq. (14). We use the same constructions and labelling as for the proof of the case $n = 3$. Thus $w = (w_1, w_2, w_3, w_4)$. Let $C = C_p(L_n(2))$. It is clear that $\dim(C) = 2^{n-1}n$ since the rows from R_1 and R_2 give dimension $2^{n-1}(n-1)$, by induction, and those from R_3 give dimension 2^{n-1} since each column has exactly one entry of 1 in it, and each row has at least one entry 1.

If w is a sum of $k \geq 1$ non-zero scalar multiples of rows r_i from R_1, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) \geq 2(n-2) + 2k$ since X has every row containing exactly two entries 1, and every column exactly one entry 1. If $k \geq 2$ then $\mathrm{wt}(w) \geq 2n$, so we only get weight $2(n-1)$ when $k = 1$. The same argument holds for w a sum of rows in R_2. If w is a sum of $k \neq 0$, non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = 2(n-1)k \geq 2(n-1)$, (since Y, Z each have their rows consisting of $n - 1$ entries equal to 1), with equality only if $k = 1$ and w is a scalar multiple of a row.

If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_2 then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 2k + 2m > 2(n-1)$. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + m(n-1) \geq 2(n-2) + \mathrm{wt}(w_3) + m(n-1) \geq 3n - 5 > 2n - 2$ for $n \geq 4$. So no weight $2(n-1)$ can arise from this combination of rows, and similarly from R_2 and R_3.

Finally we take w to be a sum of $k \neq 0$ non-zero scalar multiples of rows from R_1 and $j \neq 0$ non-zero scalar multiples of rows from R_2 and $m \neq 0$ non-zero scalar multiples of rows from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4) \geq 4(n-2) > 2n - 4$ for $n \geq 4$. This completes the proof for p odd.

Case (ii): $p = 2$

Again by Lemma 5 we have the result for $n = 3$, so we use induction. So suppose $n \geq 4$ and that it is true for $n - 1$, and consider $L_n(2)$ as shown in Eq. (14). We use the same constructions and labelling as before. Thus $w = (w_1, w_2, w_3, w_4)$. Let $C = C_2(L_n(2))$. It is clear that $\dim(C) \leq 2^{n-1}n - 1$ since the sum of all the rows is 0. Further notice that any $2^{n-1}n - 1$ rows of $L_{n-1}(2)$ are linearly independent. By induction the dimension is at least this as the rows from R_1 give dimension at least $2^{n-2}(n-1) - 1$, and the those from R_2 and R_3 give dimension $2^{n-2}(n-1)$ and 2^{n-1}, respectively, since each column has exactly one entry of 1 in it, and each row has at least one entry 1.

If w is a sum of $k \geq 1$ rows r_i from R_1, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) \geq \mathrm{wt}(w_1) + 2k$ since X has every row containing exactly two entries 1, and every column exactly one entry 1. If $w_1 = 0$ then $k = 2^{n-2}(n-1)$ and $\mathrm{wt}(w) = 2^{n-1}(n-1) > 2(n-1)$. Otherwise $\mathrm{wt}(w) \geq 2(n-2) + 2k \geq 2(n-2) + 2 = 2(n-1)$ with equality only if $k = 1$. The same argument holds for w a sum of rows in R_2. If w is a sum of $k \neq 0$, rows from R_2, then $\mathrm{wt}(w) = 2(n-1)k \geq 2(n-1)$, (since Y, Z each have their rows consisting of $n-1$ entries equal to 1), with equality only if $k = 1$ and w is a scalar multiple of a row.

If w is a sum of $k \neq 0$ rows from R_1 and $m \neq 0$ rows from R_2 then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 2k + 2m$. If $w_1 = 0$ then $k = 2^{n-2}(n-1)$ so $\mathrm{wt}(w) \geq 2^{n-1}(n-1) + 2 > 2(n-1)$ for $n \geq 4$. Similarly if $w_2 = 0$. So we can assume neither is 0, in which case $\mathrm{wt}(w) \geq 4(n-2) + 4 > 2n - 2$ for $n \geq 4$. Now take w to be a sum of $k \geq 1$ rows from R_1 and $m \geq 1$ rows from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + m(n-1)$. If $w_1 = 0$ then $k = 2^{n-2}(n-1)$ and $\mathrm{wt}(w_3) = 2^{n-1}(n-1) - m(n-1)$, so $\mathrm{wt}(w) = 2^{n-1}(n-1) > 2(n-1)$. Otherwise $\mathrm{wt}(w_1) \geq 2(n-2)$ and $\mathrm{wt}(w) \geq 2(n-2) + \mathrm{wt}(w_3) + m(n-1) \geq 3n-5 > 2n-2$ for $n \geq 4$. So no weight $2(n-1)$ can arise from this combination of rows, and similarly from R_2 and R_3.

Finally we take w to be a sum of $k \geq 1$ rows from R_1 and $j \geq 1$ rows from R_2 and $m \geq 1$ rows from R_3. Then if $w_1, w_2 \neq 0$, $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4) \geq 4(n-2) > 2n-4$ for $n \geq 4$. If $w_1 = 0, w_2 \neq 0$ then $k = 2^{n-2}(n-1)$ and $\mathrm{wt}(w_3) = 2^{n-1}(n-1) - m(n-1)$ and $\mathrm{wt}(w) \geq 2(n-2) + 2^{n-1}(n-1) - m(n-1) + \mathrm{wt}(w_4) > 2(n-1)$ unless $m = 2^{n-1}$ and $\mathrm{wt}(w_4) = 0, 2$. If $\mathrm{wt}(w_4) = 0$ then $j = 2^{n-2}(n-1)$ and $w = 0$. If $\mathrm{wt}(w_4) = 2$ then $j = 2^{n-2}(n-1) - 1$ and w is the row of R_2 that was left out of the sum. Finally, if $w_1, w_2 = 0$ then $k = j = 2^{n-2}(n-1)$, $\mathrm{wt}(w) = 2(2^{n-1} - m)(n-1) > 2(n-1)$ if $m < 2^{n-1} - 1$. If $m = 2^{n-1} - 1$ then w is the row of R_3 that was omitted from the sum, and if $m = 2^{n-1}$, then $w = 0$. This completes all cases and the induction.

For the statement about the dual codes, that the minimum weight is at most 4 follows from Lemma 4. For $p = 2$, for any $x \in R^n$, the set $\{[[x, x+e_1], [x, x+e_2]], [[x, x+e_1], [x, x+e_3]], [[x, x+e_2], [x, x+e_3]]\}$ forms the support of a word of weight 3 in the dual code.

The statement about the automorphism group of the code follows from Whitney's Theorem (see Section 3), Lemma 1, and the proof of the similar statement in Proposition 1. ■

Note. We will not consider here the general case of an incidence matrix $L_n(m)$ for $L(H(n,m))$ for $m \geq 3$, although all indications (for example, with Magma) are that similar results hold.

8. Codes from an incidence matrix for $L_2(H(n, 2))$

Recall that we write $J_n(m)$ for a $\frac{1}{2}m^n(m-1)n((m-1)n-1) \times \frac{1}{2}m^n(m-1)n((m-1)n-1)(2(m-1)n-3)$ incidence matrix for $L(L(H(n,m))) = L_2(H(n,m))$. We restrict our attention to $m = 2$, i.e. we consider the graph $L(L(H(n,2)))$. We let $J_n(2)$ be an incidence matrix for this graph, using the same ordering for the rows as for the columns of $L_n(2)$, and ordering the columns using the same algorithm as we used for $L_n(2)$. Then, from Example 1, $L_2(H(n,2))$ has valency $4n-6$ and $J_n(2)$ is $2^{n-1}n(n-1) \times 2^{n-1}n(n-1)(2n-3)$, of the form

$$J_n(2) = \left[\begin{array}{c|c|c|c|c|c|c} J_{n-1}(2) & 0 & X & 0 & 0 & 0 & 0 \\ \hline 0 & J_{n-1}(2) & 0 & W & 0 & 0 & 0 \\ \hline 0 & 0 & Y_1 & 0 & Y_2 & 0 & Y_3 \\ \hline 0 & 0 & 0 & Z_1 & 0 & Z_2 & Z_3 \end{array}\right], \qquad (16)$$

where X, W are $2^{n-2}(n-1)(n-2) \times 2^n(n-1)(n-2)$ matrices; Y_1, Z_1 are $2^{n-1}(n-1) \times 2^n(n-1)(n-2)$ matrices; Y_2, Z_2 are $2^{n-1}(n-1) \times 2^{n-2}(n-1)^2$ matrices; Y_3, Z_3 are $2^{n-1}(n-1) \times 2^{n-1}(n-1)^2$ matrices. Further, every column of X, Y_1, Y_3, Z_1, Z_3, W has exactly one non-zero entry 1 in it, and every column of Y_2, Z_2 has two non-zero entries 1 in it; every row of X and W has precisely four non-zero entries 1 in it; every row of Y_1 and Z_1 has precisely $2(n-2)$ non-zero entries 1 in it; every row of Y_2 and Z_2 has precisely $(n-1)$ non-zero entries 1 in it; every row of Y_3 and Z_3 has precisely $(n-1)$ non-zero entries 1 in it.

For example, for $n = 3$,

$$J_2(2) = \begin{bmatrix} 1 & 1 & & \\ 1 & & 1 & \\ & 1 & & 1 \\ & & 1 & 1 \end{bmatrix}, \qquad X = \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & & & & & & & \\ & & & & 1 & 1 & 1 & 1 & & & & & & & & \\ & & & & & & & & 1 & 1 & 1 & 1 & & & & \\ & & & & & & & & & & & & 1 & 1 & 1 & 1 \end{bmatrix},$$

$$Y_1 = \begin{bmatrix} 1 &&&& 1 &&&&&&&&&&& \\ & 1 &&&& 1 &&&&&&&&&& \\ && 1 &&&&&& 1 &&&&&&& \\ &&& 1 &&&&&& 1 &&&&&& \\ &&&&&& 1 &&&&&& 1 &&& \\ &&&&&&& 1 &&&&&& 1 && \\ &&&&&&&&&& 1 &&&& 1 & \\ &&&&&&&&&&& 1 &&&& 1 \end{bmatrix}, \quad Y_2 = \begin{bmatrix} 1 & 1 &&&&&& \\ 1 && 1 &&&&& \\ & 1 && 1 &&&& \\ &&& 1 & 1 &&& \\ && 1 &&& 1 && \\ &&&&& 1 & 1 & \\ &&&& 1 &&& 1 \\ &&&&&& 1 & 1 \end{bmatrix},$$

$$Y_3 = \begin{bmatrix} 1 & 1 &&&&&&&&&&&&&& \\ && 1 & 1 &&&&&&&&&&&& \\ &&&& 1 & 1 &&&&&&&&&& \\ &&&&&& 1 & 1 &&&&&&&& \\ &&&&&&&& 1 & 1 &&&&&& \\ &&&&&&&&&& 1 & 1 &&&& \\ &&&&&&&&&&&& 1 & 1 && \\ &&&&&&&&&&&&&& 1 & 1 \end{bmatrix},$$

$$W = \begin{bmatrix} 1 && 1 && 1 &&&& 1 &&&&&&& \\ & 1 &&&& 1 & 1 &&&&&& 1 &&& \\ &&& 1 &&&&&& 1 & 1 &&&& 1 & \\ &&&&&&& 1 &&&& 1 && 1 && 1 \end{bmatrix},$$

and Z_1, Z_2, Z_3 are Y_1, Y_2, Y_3, respectively.

As in Section 7, we need to establish an induction base for our proposition, and we do this in a lemma, with notation as given above.

Lemma 6. *$C_2(J_3(2)) = [72, 23, 6]_2$ and for p odd $C_p(J_3(2)) = [72, 24, 6]_p$. The vectors of weight 6 are the scalar multiples of the rows of $J_3(2)$ for all p.*

Proof. Write $J_3 = J_3(2)$. We can use Magma for $p = 2$. For p odd, we can use Result 1 for the dimension since $L(H(3, 2))$ has a path of length 5, and hence so does its line graph, by the remark in Section 5.

Label the row partitions of J_3 as in Eq. (16) as R_i for $i = 1, 2, 3, 4$ and the column partitions as C_i for $i = 1, \ldots, 7$. Then $w \in C_p(J_n)$ is a concatenation of w_i, $i = 1, \ldots, 7$.

Take p to be any prime. It is easy to see that $C_p(J_2)$ has dimension 3 and minimum weight 2. Further, writing the rows of J_2 as r_i for $1 \le i \le 4$, any three of the rows are linearly independent, and $w = \sum_{i=1}^{4} \alpha_i r_i = (\alpha_1{+}\alpha_2, \alpha_1{+}\alpha_3, \alpha_2{+}\alpha_4, \alpha_3{+}\alpha_4) = 0$ only if $\alpha_1 = \alpha_4 = -\alpha_2 = -\alpha_3$. Now we need to show that $C_p(J_3)$ has minimum weight 6 and that the words of weight 6 are the scalar multiples of the rows of J_3.

First we take w to be a sum of $k \ge 1$ non-zero scalar multiples of rows from R_1. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k$. If $w_1 = 0$ then from the above discussion we must have $k = 4$ and thus $\mathrm{wt}(w) = 16$. If $w_1 \neq 0$ then $\mathrm{wt}(w) \ge 2 + 4k \ge 6$, with equality only when $k = 1$ and we have a multiple of a row. The same argument applies to a sum of rows from R_2, since W is equivalent to X. If w is a sum of $k \ge 1$ non-zero scalar multiples of rows from R_3 or R_4, then $\mathrm{wt}(w) = 6k \ge 6$ with equality only if $k = 1$.

Now take w to be a sum of $k \ge 1$ non-zero scalar multiples of rows from R_1 and $m \ge 1$ non-zero scalar multiples of rows from R_2. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 4k + 4m > 6$. If w is a sum of $k \ge 1$ rows from R_1 and $m \ge 1$ rows from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 4m$. If $w_1 = 0$ then $k = 4$ and $\mathrm{wt}(w) = \mathrm{wt}(w_3) + 4m > 6$ if $m \ge 2$. If $m = 1$ then $\mathrm{wt}(w_3) \ge 14$ since $w_3 = x + \beta y$ where x has weight 16, and y is a row of Y_1 and has weight 2. Rows from R_2 and R_4 behave similarly. If w is a sum of $k \ge 1$ rows from R_1 and $m \ge 1$ rows from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k + 6m \ge 10$, and similarly for R_2 and R_3. For k from R_3 and m from R_4, $\mathrm{wt}(w) = 4k + 4m + \mathrm{wt}(w_7) > 6$.

Next take w to be a sum of $k \ge 1$ non-zero scalar multiples of rows from R_1, $m \ge 1$ from R_2 and $\ell \ge 1$ from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + 4m + 4\ell > 6$. If w is a sum of $k \ge 1$ from R_1, $m \ge 1$ from R_3 and $\ell \ge 1$ from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 2m + 4\ell + \mathrm{wt}(w_7) \ge 6$ with equality only if $m = \ell = 1$, $w_1 = w_3 = w_7 = 0$. But $w_1 = 0$ implies $k = 4$ and then, as before, $\mathrm{wt}(w_3) \ge 14$, which is impossible. This covers all choices of three blocks of rows, due to the symmetry of the matrix.

Finally, if w is a sum of non-zero scalar multiples of $k \ge 1$ rows from R_1, $m \ge 1$ from R_2, $\ell \ge 1$ from R_3, and $r \ge 1$ from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4) + 2\ell + 2r + \mathrm{wt}(w_7) > 6$ if both $w_1, w_2 \neq 0$. If $w_1 \neq 0$ and $w_2 = 0$ then $m = 4$, and $\mathrm{wt}(w) > 6$ unless $r = \ell = 1$, in which case $\mathrm{wt}(w_4) > 14$ which is not possible. If $w_1, w_2 = 0$, then $k = m = 4$ so $\mathrm{wt}(w) > 6$ if both $r, \ell \ge 2$. So suppose $r = 1$. Then $\mathrm{wt}(w_4) \ge 14$ again, so we have a contradiction. This completes the proof. ■

Proposition 6. *For $n \ge 2$, let $J_n(2)$ be a $2^{n-1}n(n-1) \times 2^{n-1}n(n-1)(2n-3)$ incidence matrix for $L(L(H(n, 2))) = L_2(H(n, 2))$. For $n \ge 3$,*

- *$C_2(J_n(2)) = [2^{n-1}n(n-1)(2n-3), 2^{n-1}n(n-1) - 1, 2(2n-3)]_2$;*
- *$C_p(J_n(2)) = [2^{n-1}n(n-1)(2n-3), 2^{n-1}n(n-1), 2(2n-3)]_p$ for p odd.*

For $n \ge 3$ and all p the minimum words are the scalar multiples of the rows of $J_n(2)$, and $\mathrm{Aut}(C_p(J_n(2))) = S_2 \wr S_n$.

Proof. We write $J_n = J_n(2)$. Much of the proof of this mirrors that of Proposition 5.

We proceed by induction, since we have an induction base from Lemma 6. The statement about the dimension of the codes follows immediately. For the minimum weight, we need to separate our proofs for p odd or $p = 2$, since the submatrix J_{n-1} can give $\mathrm{wt}(w_1) = 0$ when taking a collection of rows from R_1 in the case $p = 2$ but not in the case p odd.

Case (i): *p odd*

Take p odd and assume we have the result for $n-1 \geq 3$. Let $w \in C_p(J_n)$. We assume that the minimum weight of $C_p(J_{n-1})$ is $4n-10$ and the words of this weight are multiples of the rows of J_{n-1}.

First we take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k \geq 4n-10+4k \geq 4n-6$ with equality only if $k = 1$. The same argument applies to a sum of rows from R_2, since W is equivalent to X. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_3 or R_4, then $\mathrm{wt}(w) = (2(n-2)+2(n-1))k \geq 4n-6$ with equality only if $k = 1$.

Now take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 2m(n-1) \geq 4n-10+2(n-1) > 4n-6$ for $n > 3$. Rows from R_2 and R_4 behave similarly. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k + m(4n-6) > 4n-6$, and similarly for R_2 and R_3. For $k \geq 1$ rows from R_1 and $m \geq 1$ from R_2 we have $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 4k + 4m \geq 2(4n-10) + 4(k+m) > 4n-6$; for k from R_3 and m from R_4, $\mathrm{wt}(w) = (2(n-2)+(n-1))k + (2(n-2)+(n-1))m + \mathrm{wt}(w_7) \geq 6n-10 > 4n-6$ for $n > 2$.

Next take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $m \geq 1$ from R_3 and $\ell \geq 1$ from R_4. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + (n-1)m + (3n-5)\ell + \mathrm{wt}(w_7) \geq 4n-10+(n-1)+(3n-5) > 4n-6$ for $n \geq 3$. If w is a sum of non-zero scalar multiples of $k \geq 1$ rows from R_1, $\ell \geq 1$ from R_2, and $m \geq 1$ from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + (2n-2)m + 4\ell \geq 2(4n-10) + 2n-2 > 4n-6$ for $n > 3$.

Finally, if w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $m \geq 1$ from R_2, $\ell \geq 1$ from R_3, and $r \geq 1$ from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4) + (n-1)\ell + (n-1)r + \mathrm{wt}(w_7) \geq 2(4n-10) + 2(n-1) > 4n-6$ for $n > 3$. This completes the proof for p odd.

Case (ii): $p = 2$

For $p = 2$ the argument needs to include the possibility that w_1 or w_2 is 0, in which case w_3 or w_4 is the all-one vector of length $2^n(n-1)(n-2) > 4n-6$ for $n \geq 3$. Again this only happens if all the rows from R_1 or R_2 are taken. Assume we have the result for $n-1 \geq 3$. Let $w \in C_2(J_n)$. We assume that the minimum weight of $C_2(J_{n-1})$ is $4n-10$ and the words of this weight are multiples of the rows of J_{n-1}. Note that J_{n-1} has $2^{n-2}(n-1)(n-2)$ rows and that the number of columns of X is $2^n(n-1)(n-2) > 4n-6$ for $n \geq 3$.

First we take w to be a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1. Then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k \geq 4n-10+4k \geq 4n-6$ with equality only if $k = 1$, unless $w_1 = 0$, in which case $k = 2^{n-2}(n-1)(n-2)$. Then $\mathrm{wt}(w) = 2^n(n-1)(n-2) > 4n-6$ for $n \geq 3$. The same argument applies to a sum of rows from R_2, since W is equivalent to X. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_3 or R_4, then $\mathrm{wt}(w) = (2(n-2)+2(n-1))k \geq 4n-6$ with equality only if $k = 1$.

If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_3 then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + 2m(n-1) \geq 4n-10+2(n-1) > 4n-6$ for $n > 3$ if $w_1 \neq 0$. If $w_1 = 0$ then $k = 2^{n-2}(n-1)(n-2)$, and if $m \geq 2$ then $\mathrm{wt}(w) \geq 4(n-1) > 4n-6$. Thus $m = 1$ and $\mathrm{wt}(w_3) = 2^n(n-1)(n-2) - 2(n-2)$, so $\mathrm{wt}(w) = 2^n(n-1)(n-2) - 2(n-2) + 2(n-1) > 4n-6$ for $n \geq 3$. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1 and $m \geq 1$ non-zero scalar multiples of rows from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + 4k + m(4n-6) > 4n-6$, and similarly for R_2 and R_3. For $k \geq 1$ rows from R_1 and $m \geq 1$ from R_2 we have $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + 4k + 4m \geq 2(4n-10) + 4(k+m) > 4n-6$ if $w_1, w_2 \neq 0$, and, should one of these be 0, then w_3 or w_4 is the all-one vector and, by the observation above, $\mathrm{wt}(w) > 4n-6$. For $k \geq 1$ from R_3 and $m \geq 1$ from R_4, $\mathrm{wt}(w) = (2(n-2)+(n-1))k + (2(n-2)+(n-1))k + \mathrm{wt}(w_7) \geq 6n-10 > 4n-6$ for $n > 2$.

If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $\ell \geq 1$ from R_2 and $m \geq 1$ from R_3, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + (2n-2)m + 4\ell \geq 2(4n-10) + 2n-2 > 4n-6$ for $n > 3$ if $w_1, w_2 \neq 0$. If $m \geq 2$ then $\mathrm{wt}(w) > 4n-6$, so $m = 1$, and if $w_1 = 0$ then $\mathrm{wt}(w) \geq \mathrm{wt}(w_3) = 2^n(n-1)(n-2) - 2(n-2) > 4n-6$, and if $w_2 = 0$ then $\ell = 2^{n-2}(n-1)(n-2)$ and $\mathrm{wt}(w) \geq 4\ell > 4n-6$. If w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $m \geq 1$ from R_3 and $\ell \geq 1$ from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_3) + (n-1)m + (3n-5)\ell + \mathrm{wt}(w_7) > 4n-6$ unless $m = \ell = 1$, in which case $\mathrm{wt}(w) \geq 4n-10+(n-1)+(3n-5)$ if $w_1 \neq 0$, and if $w_1 = 0$, then $\mathrm{wt}(w_3) = 2^n(n-1)(n-2) - 2(n-2) > 4n-6$ for $n \geq 3$.

Finally, if w is a sum of $k \geq 1$ non-zero scalar multiples of rows from R_1, $r \geq 1$ from R_2, $m \geq 1$ from R_3, and $\ell \geq 1$ from R_4, then $\mathrm{wt}(w) = \mathrm{wt}(w_1) + \mathrm{wt}(w_2) + \mathrm{wt}(w_3) + \mathrm{wt}(w_4) + (n-1)m + (n-1)\ell + \mathrm{wt}(w_7) \geq 2(4n-10) + 2(n-1) > 4n-6$ for $n > 3$ if $w_1, w_2 \neq 0$. If $m + \ell \geq 4$ then $\mathrm{wt}(w) > 4n-6$, so take $2 \leq m + \ell \leq 3$. If $w_1 = 0$ then $\mathrm{wt}(w_3) = 2^n(n-1)(n-2) - 2m(n-2) \geq 2^n(n-1)(n-2) - 4(n-2) > 4n-6$ for $n \geq 3$. Similarly if $w_2 = 0$. This completes the proof.

The statement about the automorphism group of the code follows from Whitney's Theorem (see Section 3), Lemma 1, and the proof of the similar statement in Proposition 1. ■

Note. All indications are that the codes from the incidence matrices $J_n(m)$ of $L_2(H(n, m))$ for $m \geq 3$ follow the same pattern, but we have not attempted a proof, there being too many variations to consider.

9. Permutation decoding

In [11, Lemma 7] the following was proved:

Result 2. *Let C be a code with minimum distance d, $\mathcal{I}$ an information set, $\mathcal{C}$ the corresponding check set and $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. Let A be an automorphism group of C, and n the maximum of $|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|$, where $\mathcal{O}$ is a A-orbit. If $s = \min\left(\left\lceil \frac{1}{n} \right\rceil - 1, \left\lfloor \frac{d-1}{2} \right\rfloor\right)$, then A is an s-PD-set for C.*

Note that this result is true for any information set. If the group A is transitive then $|\mathcal{O}|$ is the degree of the group and $|\mathcal{O} \cap \mathcal{I}|$ is the dimension of the code.

If we take $C = C_p(G_n(m))$, the degree is $\frac{1}{2}m^n(m-1)n$ and the dimension is $m^n - 1$. Certainly the group $S_m \wr S_n$ is transitive, and has transitive subgroups. One of the smallest order should be taken to minimize the size of the PD-set. If this is done then $C_p(G_n(m))$ can be used to its full error-correction capability with this group as PD-set since in all cases s in Result 2 is $\left\lfloor \frac{(m-1)n-1}{2} \right\rfloor$.

For example, if $R = \mathbb{Z}_m$, then if

$$T_{a_1,\ldots,a_n} : (x_1, \ldots, x_n) \mapsto (x_1 + a_1, \ldots, x_n + a_n)$$

mapping $\mathbb{Z}_m^n$ to itself, and if, for $a \in \mathbb{Z}_m^*$, $\sigma = (1, \ldots, n) \in S_n$, acting as a permutation matrix on $\mathbb{Z}_m^n$, then

$$A = \{T_x \mid x \in \mathbb{Z}_m^n\}\{b\sigma^i \mid b \in \mathbb{Z}_m^*, 1 \leq i \leq n\}$$

is a transitive subgroup group of order $m^n(m-1)n$. This follows since if $P = [0, ae_1]$, $Q = [x, x + be_j]$, where $a, b \neq 0$, $a, b \in \mathbb{Z}_m$, then $\tau = a^{-1}b\sigma^j T_{x_1,\ldots,x_n}$ will have $P\tau = Q$.

We take $m > 2$ here since $m = 2$ has been covered in [6].

Proposition 7. *For $n \geq 3$, $m \geq 3$ any transitive subgroup of $S_m \wr S_n$ of degree $\frac{1}{2}m^n(m-1)n$ is a PD-set for the code $C_p(G_n(m))$, where $C_2(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n - 1, (m-1)n\right]_2$ and $C_p(G_n(m)) = \left[\frac{1}{2}m^n(m-1)n, m^n, (m-1)n\right]_p$ for p odd, for any information set.*

Proof. We use Result 2 and the propositions and lemmas we have obtained for the dimensions of the codes and their minimum weights. ■

The proof of Theorem 1 now follows from the propositions in the preceding sections.

10. Further classes of graphs

The codes from the incidence matrices of line graphs $L_i(H(n, m))$ for $i \geq 1$ and $m \geq 3$, or for $i \geq 3$ and $m \geq 2$, behave similarly in all cases where we have tested them computationally. However they become too large and complicated to handle in a manner similar to the one we have employed in this paper, so a more general approach might be needed for these.

The definition of the Hamming graphs $H(n, m)$ can be extended to the class of graphs $H^k(n, m)$, for $k, n, m \geq 1$, i.e. the graphs with vertices the $m^n n$-tuples in R^n, and adjacency defined by two vertices in R^n being adjacent if they differ in k coordinate positions. (These are the graphs in the Hamming association scheme.) We can examine codes from an $m^n \times \frac{1}{2}m^n(m-1)^k \binom{n}{k}$ incidence matrix for $H^k(n, m)$ and also the incidence matrices of their line graphs. These codes appear to share properties similar to those we mentioned in Section 1 and that we have established here for the $H(n, m)$. Computations with Magma confirm this. We examine these codes in a forthcoming paper.

Acknowledgement

J.D. Key thanks the Department of Mathematics and Applied Mathematics at the University of the Western Cape for their hospitality.

References

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

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (3/4) (1997) 235–265.

[3] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, in: Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3, Band 18, Springer-Verlag, Berlin, New York, 1989.

[4] J. Cannon, A. Steel, G. White, Linear codes over finite fields, in: J. Cannon, W. Bosma (Eds.), Handbook of Magma Functions, Computational Algebra Group, Department of Mathematics, University of Sydney, V2.13, 2006, pp. 3951–4023. http://magma.maths.usyd.edu.au/magma.

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

[6] W. Fish, J.D. Key, E. Mwambene, Binary codes of line graphs from the *n*-cube, J. Symbolic Comput. (in press).

[7] W. Fish, J.D. Key, E. Mwambene, Graphs, designs and codes related to the *n*-cube, Discrete Math. 309 (2009) 3255–3269.

[8] W. Fish, J.D. Key, E. Mwambene, Codes, designs and groups from the Hamming graphs, J. Comb. Inf. Syst. Sci. 34 (1–4) (2009) 169–182.

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

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

[11] J.D. Key, T.P. McDonough, V.C. Mavron, Information sets and partial permutation decoding for codes from finite geometries, Finite Fields Appl. 12 (2006) 232–247.

[12] J.D. Key, J. Moori, B.G. Rodrigues, Codes associated with triangular graphs, and permutation decoding, Int. J. Inform. and Coding Theory (in press).
[13] J.D. Key, B.G. Rodrigues, Codes associated with lattice graphs, and permutation decoding (submitted for publication).
[14] J.D. Key, B.G. Rodrigues, Codes from incidence matrices of strongly regular graphs (in preparation).
[15] Hans-Joachim Kroll, Rita Vincenti, PD-sets related to the codes of some classical varieties, Discrete Math. 301 (2005) 89–105.
[16] F.J. MacWilliams, Permutation decoding of systematic codes, Bell Syst. Tech. J. 43 (1964) 485–505.
[17] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.
[18] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.
[19] Hassler Whitney, Congruent graphs and the connectivity of graphs, Amer. J. Math. 54 (1932) 154–168.