Linear codes from designs from Hamming graphs

J. D. Key

Clemson University (SC, USA)
Aberystwyth University (Wales, UK)
University of KwaZulu-Natal (South Africa)
University of the Western Cape (South Africa)

keyj@clemson.edu
www.math.clemson.edu/~keyj

April 13, 2010
Abstract

The Hamming graph $H^k(n, m)$, for $n, k, m$ integers, $1 \leq k < n$, 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 $k$ coordinate positions. They are the graphs from the Hamming association scheme. In particular, the $n$-cube: $Q_n = H(n, 2) = H^1(n, 2)$ ($R = \mathbb{F}_2$).

We examine the $p$-ary codes, for $p$ any prime, that can be obtained from incidence and neighbourhood designs from $H^k(n, m)$ and its line graphs.

For the incidence designs we obtain the main parameters, including the minimum weight and nature of the minimum words, for all $m$ when $k = 1$, and for $m = 2$ when $k \geq 2$. The automorphism groups of the graphs, designs and codes are obtained for these parameters, and permutation decoding shown to be applicable. Joint work with W. Fish and E. Mwambene of University of the Western Cape.
The general idea

Codes from the **row** span of **incidence matrices** of some classes of graphs share certain useful properties:

\[ \Gamma = (V, E) \] regular connected graph of valency \( k \), and \( |V| = N \);
\( G \) an \( N \times \frac{1}{2} Nk \) **incidence matrix** (vertices by edges) for \( \Gamma \);
\( C_p(G) \) the code spanned by the rows of \( G \) over \( \mathbb{F}_p \), for \( p \) prime, might be

\[ \left[ \frac{1}{2}Nk, N, k \right]_p \] or \[ \left[ \frac{1}{2}Nk, N - 1, k \right]_2, \]

with **minimum vectors** the scalar multiples of the rows of \( G \).
There is often a gap in the weight enumerator between $k$ and $2(k - 1)$, the latter arising from the difference of two rows (when $p = 2$ the code of the adjacency matrix of the line graph). See: [KMR10, KRa, KRb]

This gap occurs for the $p$-ary code of the desarguesian projective plane $PG_2(\mathbb{F}_q)$, where $q = p^t$; also for other designs from desarguesian geometries $PG_{n,k}(\mathbb{F}_q)$. See [Cho00, LSdV08a, LSdV08b]

But, not always true for non-desarguesian planes: e.g. there are planes of order 16 that have words in this gap. See [GdRK08]. (This has also shown that there are affine planes of order 16 whose binary code has words of weight 16 that are not incidence vectors of lines.)
1. Background and terminology
2. Codes from incidence matrices of graphs
3. Hamming graphs $H(n, m)$
4. Hamming graphs $H^k(n, m)$
5. Incidence designs for $H^k(n, m)$
6. Codes of incidence designs of $H^k(n, m)$
7. Automorphism groups
8. Codes from adjacency matrices
9. References
The **graphs**, $\Gamma = (V, E)$ with vertex set $V$, $N = |V|$, and edge set $E$, are undirected with no loops.

- If $x, y \in V$ and $x$ and $y$ are adjacent, $x \sim y$, and $[x, y]$ is the edge they define.
- A graph is **regular** if all the vertices have the same valency $k$.
- An **adjacency matrix** $A = [a_{i,j}]$ of $\Gamma$ is an $N \times N$ matrix with $a_{i,j} = 1$ if vertices $v_i \sim v_j$, and $a_{i,j} = 0$ otherwise.
- 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 **$t$-$(v, k, \lambda)$ 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 $\lambda$ blocks.
The **neighbourhood design** $\mathcal{D}(\Gamma)$ of a regular graph $\Gamma$ is the $1-(N, k, k)$ symmetric design with points the vertices of $\Gamma$ and blocks the sets of neighbours of a vertex, for each vertex, i.e. an adjacency matrix of $\Gamma$ is an incidence matrix for $\mathcal{D}$.

An **incidence matrix** of $\Gamma$ is an $N \times |E|$ matrix $B$ with $b_{i,j} = 1$ if the vertex labelled by $i$ is on the edge labelled by $j$, and $b_{i,j} = 0$ otherwise.

If $\Gamma$ is regular with valency $k$, then $|E| = \frac{Nk}{2}$ and the $1-(\frac{Nk}{2}, k, 2)$ design with incidence matrix $B$ is called the **incidence design** $\mathcal{G}(\Gamma)$ of $\Gamma$.

The **line graph** $L(\Gamma)$ of $\Gamma = (V, E)$ is the graph with vertex set $E$ and $e$ and $f$ in $E$ are adjacent in $L(\Gamma)$ if $e$ and $f$ as edges of $\Gamma$ share a vertex in $V$. 
Terminology and definitions continued

- The **code** $C_F(D)$ of the design $D$ over a field $F$ is the space spanned by the incidence vectors of the blocks over $F$.

- For $X \subseteq P$, the **incidence vector** in $F^P$ of $X$ is $v^X$.

- The **code** $C_F(\Gamma)$ or $C_p(A)$ of graph $\Gamma$ over $F_p$ is the row span of an adjacency matrix $A$ over $F_p$. So $C_p(\Gamma) = C_p(D(\Gamma))$ if $\Gamma$ is regular.

- If $B$ is an incidence matrix for $\Gamma$, $C_p(B)$ denotes the row span of $B$ over $F_p$. So $C_p(B) = C_p(G(\Gamma))$ if $\Gamma$ is regular.

- If $A$ is an adjacency matrix and $B$ an incidence matrix for $\Gamma$, $M$ is an adjacency matrix for $L(\Gamma)$, $\Gamma$ regular of valency $k$, $N$ vertices, $e$ edges, then

  \[ BB^T = A + kl_N \quad \text{and} \quad B^T B = M + 2l_e. \]
A **linear code** is a subspace of a finite-dimensional vector space over a finite field. (All codes are linear in this talk.)

The **weight** of a vector $v$, written $\text{wt}(v)$, is the number of non-zero coordinate entries. If a code has smallest non-zero weight $d$ then the code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors by nearest-neighbour decoding.

A code $C$ is $[n, k, d]_q$ if it is over $\mathbb{F}_q$ and of length $n$, dimension $k$, and minimum weight $d$.

A **generator matrix** for the code is a $k \times n$ matrix made up of a basis for $C$.

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 $H$ for $C^\perp$.

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 $C$.

Any code is isomorphic to a code with generator matrix in standard form, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first $k$ coordinates are the information symbols and the last $n - k$ coordinates are the check symbols.
Result

\( \Gamma = (V, E) \) is a graph, \( G \) an incidence matrix, \( \mathcal{G} \) the incidence design, \( C_p(G) \) the row-span of \( G \) over \( \mathbb{F}_p \).

1. If \( \Gamma \) is connected then \( \dim(C_2(G)) = |V| - 1 \).

2. If \( \Gamma \) is connected and has a closed path of odd length \( \geq 3 \), then \( \dim(C_p(G)) = |V| \) for \( p \) odd.

3. If \([P, Q, R, S]\) is a closed path in \( \Gamma \), then for any prime \( p \),

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

4. If \( \Gamma \) is regular, \( \text{Aut}(\Gamma) = \text{Aut}(\mathcal{G}) \).
(From [KRb])
That $\dim(C_p(G)) \geq |V| - 1$ is folklore and easy to prove. Clearly there is equality for $p = 2$.
For $p$ odd, let $w = \sum a_i r_i = 0$ be a sum of multiples of the rows $r_i$ of $G$, where $r_i$ corresponds to the vertex $i$.
If $[i,j]$ is an edge then $a_i = -a_j$. Taking a closed path $(i_0, i_1, \ldots i_m)$ of odd length, so $a_{i_0} = -a_{i_1} = \ldots = a_{i_m} = -a_{i_0}$, and thus $a_{i_0} = 0$.
Since the graph is connected, we thus get $a_i = 0$ for all $i$.

Proof of (3) immediate, and of (4) quite direct.
Hamming graphs $H(n, m)$

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

$$x \sim y \text{ if } d(x, y) = 1$$

- Valency is $(m - 1)n$;
- Number of edges is $\frac{1}{2}m^n(m - 1)n$.
- Edges are $[x, y]$ where $d(x, y) = 1$, or $[x, x + e]$ where $x, e \in R^n$ and $\text{wt}(e) = 1$ if we take $R$ to be a ring;
- $\text{Aut}(H(n, m)) = S_m \wr S_n$ (see [BCN89]), where $S_n$ is the symmetric group on the $n$ coordinate positions of $R^n$ acting on the $n$-tuples, and $S_m$ acts on the elements of $R$.

By Whitney [Whi32],

$$\text{Aut}(L(H(n, m))) = \text{Aut}(H(n, m)) = S_m \wr S_n.$$ 

For convenience, take $R$ to be a commutative ring.
\( \mathcal{D}_n(m) \) is the \( 1-(m^n, (m-1)n, (m-1)n) \) symmetric neighbourhood design with blocks

\[
\bar{x} = \{ y \mid y \in R^n, d(x, y) = 1 \} = \{ x + e \mid \text{wt}(e) = 1 \},
\]

for \( x \in R^n \) if \( R \) is a ring.

\( G_n(m) \) is an \( m^n \times \frac{1}{2} m^n(m-1)n \) incidence matrix for \( H(n, m) \) and \( \mathcal{G}_n(m) \) the incidence design, with blocks

\[
\bar{x} = \{ [x, y] \mid d(y, y) = 1 \} = \{ [x, x + e] \mid e \in R^n, \text{wt}(e) = 1 \},
\]

for \( x \in R^n \) if \( R \) is a ring.

\( \mathcal{G}_n(m) \) is a \( 1-(\frac{1}{2} m^n(m-1)n, (m-1)n, 2) \) design.
The Hamming graphs $H^k(n, m)$, where $k, n, m \geq 1$ are integers:

- vertex set $R^n$;
- $x \sim y$ if $d(x, y) = k$, so $[x, x + e]$ where $\text{wt}(e) = k$;
- valency is $(m - 1)^k \binom{n}{k}$;
- $G^k_n(m)$ is an $m^n \times \frac{1}{2} m^n (m - 1)^k \binom{n}{k}$ incidence matrix;
- $G^k_n(m)$ is the $1-(\frac{1}{2} m^n (m - 1)^k \binom{n}{k}, \binom{n}{k}, 2)$ incidence design;
- $D^k_n(m)$ is the $1-(m^n, (m - 1)^k \binom{n}{k}, (m - 1)^k \binom{n}{k})$ neighbourhood design, and is symmetric.

($H^1(n, m) = H(n, m)$)
The block of the design $\mathcal{D}_n^k(m)$ defined by $x \in R^n$ is $\bar{x}_k$, where

$$\bar{x}_k = \{y \mid y \in R^n, \text{wt}(x - y) = k\} = \{x + e \mid \text{wt}(e) = k\}.$$

Note that $\mathcal{D}_n^k(2) = \mathcal{D}_n^{n-k}(2)$.

The block of the design $\mathcal{G}_n^k(m)$ defined by $x \in R^n$ is $\bar{x}_k$, where

$$\bar{x}_k = \{[x, x + e] \mid e \in V_n, \text{wt}(e) = k\}.$$

(So $\bar{x}_1 = \bar{x}$ and $\bar{x}_1 = \bar{x}$.)
An incidence matrix $G_n(m)$ for $H(n, m)$:

$$
\begin{bmatrix}
G_{n-1}(m) & 0 & 0 & 0 & \cdots & I & I & I & \cdots & 0 & 0 & 0 \\
0 & G_{n-1}(m) & 0 & 0 & \cdots & I & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & G_{n-1}(m) & 0 & \cdots & 0 & I & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & G_{n-1}(m) & \cdots & 0 & 0 & I & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & G_{n-1}(m) & 0 & 0 & 0 & \cdots & 0 & I & I \\
\end{bmatrix},
$$

where $I = I_{m^{n-1}}$ and there are $m - 1$ of them in each of the $m$ sets $R_i$ of rows.

There are $\binom{m+1}{2}$ column blocks.

There are $m$ column blocks $C_i$ for which the only entry is $G_{n-1}$, and these are the first $m$ column blocks, $C_1, \ldots, C_m$. 
Incidence matrices for $H(n, 2)$ and $H(n, 3)$

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

$$G_n(2) = \begin{bmatrix} G_{n-1}(2) & 0 & I \\ 0 & G_{n-1}(2) & I \end{bmatrix},$$

$$G_n(3) = \begin{bmatrix} G_{n-1}(3) & 0 & 0 & I & I & 0 \\ 0 & G_{n-1}(3) & 0 & I & 0 & I \\ 0 & 0 & G_{n-1}(3) & 0 & I & I \end{bmatrix},$$

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

J. D. Key
Linear codes from designs from Hamming graphs
For $G_n^k = G_n^k(2)$, a $2^n \times 2^{n-1}\binom{n}{k}$ incidence matrix for $H^k(n, 2)$,

$$G_n^k = \begin{bmatrix}
G_n^{k-1} & 0 & 0 & A & C & 0 \\
0 & 0 & A & 0 & 0 & C \\
0 & B & 0 & D & 0 \\
0 & G_n^{k-1} & 0 & B & 0 & D
\end{bmatrix},$$

where

- $A, B$ are $2^{n-2} \times 2^{n-1}\binom{n-2}{k-2}, \binom{n-2}{k-2}$ entries 1 in each row,
- $C, D$ are $2^{n-2} \times 2^{n-1}\binom{n-2}{k-2}, \binom{n-2}{k-2}$ entries 1 in each row,
- $A, B, C, D$ have precisely one entry 1 in each column.
For $k$ even, $H^k(n, 2)$ is not connected. Starting with $n = 2$, list the rows with the even-weight vectors for the first $2^{n-1}$ rows, $R_1$, and the odd weight vectors for the second set, $R_2$.

Obtain a $2^n \times 2^{n-1} \binom{n}{k}$ incidence matrix $G_n^k$ for $H^k(n, 2)$ for $n \geq 3$, each row of weight $\binom{n}{k}$, that can take the form

$$G_n^k = \begin{bmatrix}
G_{n-1}^k & G_{n-1}^{k-1} & 0 & 0 \\
0 & 0 & G_{n-1}^k & G_{n-1}^{k-1}
\end{bmatrix},$$

where

- $G_{n-1}^k$ is $2^{n-1} \times 2^{n-2} \binom{n-1}{k}$ with each row of weight $\binom{n-1}{k}$;
- $G_{n-1}^{k-1}$ is $2^{n-1} \times 2^{n-2} \binom{n-1}{k-1}$ with each row of weight $\binom{n-1}{k-1}$. 

Incidence matrix $G_3^2(2)$ for $H^2(3, 2)$

E.g., $n = 3, k = 2$:

$$G_3^2(2) = \begin{bmatrix}
G_2^2(2) & G_2(2) & 0 & 0 \\
0 & 0 & G_2^2(2) & G_2(2)
\end{bmatrix}.$$

$$= \begin{bmatrix}
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\end{bmatrix},$$

the rows labelled by $(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)$ for the even-weight vectors, followed by $(0, 0, 1), (1, 1, 1), (1, 0, 0), (0, 1, 0)$ for the odd.
From Result 1, with $\Gamma = H^k(n, m)$:
for $n, m \geq 2$, $n > k$, all primes $p$, $C_p(G^k_n(m))^\perp$ contains the weight-4 word

$$v[x,x+e] - v[x,x+f] - v[x+e+f,x+e] + v[x+e+f,x+f],$$

where $x \in R^n$, $\text{wt}(e) = \text{wt}(f) = k$, $e \neq f$.

$C_p(G^k_n(m))^\perp$ has minimum weight 4 for $p$ odd, any $m$, and for $p = 2 = m$;
$C^k_2(G_n(m))^\perp$ has minimum weight 3 for $m \geq 3$. 
Theorem ([FKMc])

- For \( n \geq 1, m \geq 3, \)
  \[ C_2(G_n(m)) = \left[ \frac{1}{2} m^n(m - 1)n, m^n - 1, (m - 1)n \right]_2; \]
  \[ C_p(G_n(m)) = \left[ \frac{1}{2} m^n(m - 1)n, m^n, (m - 1)n \right]_p \text{ for } p \text{ odd}. \]

- For \( m = 2, p \text{ any prime}, \)
  \[ C_p(G_n(2)) = \left[ 2^{n-1}n, 2^n - 1, n \right]_p. \]

- For \( n \geq 2, \text{ all } p \text{ and } m \geq 3, \text{ and for } n \geq 3 \text{ and } m = 2, \) 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 \( p \text{ odd, any } m, \text{ and for } p = 2 = m. \)
Codes of incidence matrices $G_n^k(2)$ of $H^k(n, 2)$

Taking $m = 2$, $G_n^k(2)$ an incidence matrix for $H^k(n, 2)$,

**Theorem**

For $n \geq 4$, $k \geq 2$,

1. For $k$ odd,
   
   $C_p(G_n^k(2)) = [2^{n-1}(\binom{n}{k}), 2^n - 1, \binom{n}{k}]_p$ for all $p$,

2. For $k$ even,
   
   $C_2(G_n^k(2)) = [2^{n-1}(\binom{n}{k}), 2^n - 2, \binom{n}{k}]_2$;
   $C_p(G_n^k(2)) = [2^{n-1}(\binom{n}{k}), 2^n, \binom{n}{k}]_p$ for $p$ odd.

The minimum words are the scalar multiples of the rows of $G_n^k(2)$. 
Codes from adjacency matrices of line graphs

\( \Gamma = (V, E) \), \( D(\Gamma) \) its neighbourhood design.

\([P, Q] \in E\) is a point of the line graph \( L(\Gamma) \) and \([P, Q]\) is a block of \( D(L(\Gamma))\):

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

**Lemma**

Let \( \Gamma \) be a graph and \([P, Q, R, S]\) a closed path in \( \Gamma \), \( p \) an odd prime. Then

\[
\]

**Proof:**

\[
\]

J. D. Key

Linear codes from designs from Hamming graphs
So codes of adjacency matrices of line graphs (of graphs with closed paths of length 4) over $\mathbb{F}_p$ for $p$ odd have minimum weight at most 4, and are not of much interest.

Recall: if $G$ is an incidence matrix for $\Gamma$, $M$ an adjacency matrix for $L(\Gamma)$ then $G^T G = M + 2I_e$.

So $C_2(M) \subseteq C_2(G)$, and is spanned by the differences of pairs of rows of $G$. 
$C_2(L(H(n, m)))$

$M_n(m)$ an adjacency matrix for $L(H(n, m))$, $G_n(m)$ an incidence matrix for $H(n, m)$, $E_n = \langle r_i - r_j \mid i \neq j, r_i, r_j, \text{rows of } G_n(m) \rangle$,

**Result ([FKMb, FKMc])**

- **For** $n \geq 2$, $C_2(M_n(2)) = E_n$, and
  \[ C_2(M_n(2)) = [2^{n-1}n, 2^n - 2, 2(n-1)]_2. \]

  For $n \geq 4$ the minimum words are the rows of $M_n(2)$, i.e. the differences of rows of $G_n(2)$.

- **For** $n \geq 2$ and for $m$ odd, $C_2(M_n(m)) = C_2(G_n(m))$, and
  \[ C_2(M_n(m)) = \left[ \frac{1}{2} m^n(m-1)n, m^n - 1, (m-1)n \right]_2 \]

  The minimum words are the rows of $G_n(m)$. 
Note that the set of supports of the words of weight 4 in the dual code form the blocks of a 1-design, and the way these meet a word in the code can be used to obtain the minimum weight and the nature of the minimum-weight vectors.
How do the automorphism groups of
- the graphs \((\Gamma)\),
- the incidence designs \((\mathcal{G})\),
- the neighbourhood designs \((\mathcal{D})\),
- and the various codes \((C)\)
fit together?

Clearly

\[
\text{Aut}(\Gamma) \subseteq \text{Aut}(\mathcal{D}) \subseteq \text{Aut}(C(\mathcal{D}))
\]

and

\[
\text{Aut}(\Gamma) \subseteq \text{Aut}(\mathcal{G}) \subseteq \text{Aut}(C(\mathcal{G})).
\]

From Result 1, for \(\Gamma\) regular, \(\text{Aut}(\Gamma) = \text{Aut}(\mathcal{G})\).
Automorphism Groups for $H(n, m)$

From [BCN89],
$\text{Aut}(H(n, m)) \cong S_m \wr S_n$, or $T \rtimes S_n$ for $H(n, 2)$,
where $T$ is the translation group on $\mathbb{R}^n$.

If $A_n$ is an adjacency matrix for $H(n, m)$, $A^*_n = A_n + I$, then

- $\mathcal{D}_n(m)$ is $1-(m^n, (m - 1)n, (m - 1)n)$ design with incidence matrix $A_n$ and blocks
  \[ \bar{x} = \{ y \mid y \in \mathbb{R}^n, d(x, y) = 1 \}, \]
  for each $x \in \mathbb{R}^n$.

- $\mathcal{D}_n(m)^*$ is $1-(m^n, (m - 1)n + 1, (m - 1)n + 1)$ design with incidence matrix $A^*_n$ and blocks
  \[ \bar{x}^* = \{ y \mid y \in \mathbb{R}^n, d(x, y) = 1 \} \cup \{ x \} = \bar{x} \cup \{ x \}, \]
  for each $x \in \mathbb{R}^n$. 
Automorphism Groups for $D_n(m)$ for $m > 2$

Result ([FKM09a])

For $n \geq 2$, $m \neq 2$,

$$\text{Aut}(D_n(m)) = \text{Aut}(D_n(m)^*) = \text{Aut}(H(n, m)) \cong S_m \wr S_n.$$  

Further, $\text{Aut}(D_n(m))$ acts primitively on the points $R^m$. 

J. D. Key

Linear codes from designs from Hamming graphs
Automorphism Groups for $H^k(n, 2)$

Taking $m = 2$, we write $\Gamma_n^k = H^k(n, 2)$, $\mathcal{D}_n^k = \mathcal{D}_n^k(2)$.

**Result ([FKM09b],[FKMd])**

For $n \geq 8$,

- $\text{Aut}(\mathcal{D}_n^1) = \text{Aut}(\mathcal{D}_n^2) = \text{Aut}(\mathcal{D}_n^3) = \text{Aut}(\Gamma_n^2) = (T^* \rtimes S_n) \wr S_2$, where $T^*$ is the group of translations by even-weight vectors of $\mathbb{F}_2^n$;
- $\text{Aut}(\Gamma_n^3) = \text{Aut}(\Gamma_n^1) = T \rtimes S_n$, where $T$ is the translation group on $\mathbb{F}_2^n$;
- For any $n$, $\text{Aut}(\mathcal{D}_n^1) \subseteq \text{Aut}(\mathcal{D}_n^k)$ for all $1 \leq k < n$. 
Automorphism Groups for $H^k(n, 2)$

<table>
<thead>
<tr>
<th>Conjecture</th>
<th>Description</th>
</tr>
</thead>
</table>
| [FKM]d | For $n \geq 2k + 2$,
| 1 | for any $k$
| \begin{align*}
\text{Aut}(D^k_n) &= \text{Aut}(D^1_n) = (T^* \rtimes S_n) \ltimes S_2;
\end{align*} |
| 2 | for $k \geq 2$ even,
| \begin{align*}
\text{Aut}(\Gamma^k_n) &= \text{Aut}(D^1_n) = (T^* \rtimes S_n) \ltimes S_2;
\end{align*} |
| 3 | for $k$ odd,
| \begin{align*}
\text{Aut}(\Gamma^k_n) &= \text{Aut}(\Gamma^1_n) = T \rtimes S_n.
\end{align*} |
Proof: Mostly done for (1) and (2).... loose ends exist!
For (1) need to show that for \( n \geq 2k + 2 \),
\[
\binom{2k}{k} \neq \binom{2m}{m} \binom{n - 2m}{k - m},
\]
for any \( m \) such that \( 1 \leq m \leq k - 1 \).
If \( f(n, m, k) = \binom{2m}{m} \binom{n - 2m}{k - m} - \binom{2k}{k} \), by Magma for \( 2 \leq k \leq 100 \),
and \( 1 \leq m \leq k - 1 \), \( f(n, m, k) \), as a polynomial in \( n \), has no
integral roots \( \geq 2k + 2 \).
For (2), we need to show that
\[
\binom{2t}{t} \binom{n - 2t}{k - t} \neq \binom{k}{k/2} \binom{n - k}{k/2}
\]
for \( 1 \leq t \leq k \), \( n \geq 2k + 2 \), unless \( t = k/2 \). Need show that all
roots of the polynomial \( N(t, n) - N(n) \) in \( n \) are less than \( 2k + 2 \),
where \( N(t, n) = \binom{2t}{t} \binom{n - 2t}{k - t} \), \( N(n) = \binom{k}{k/2} \binom{n - k}{k/2} \).
Some elements of $\text{Aut}(\mathcal{D}_n^k)$ not in $T \rtimes S_n$

For (3), can show that $\text{Aut}(\Gamma_n^k) < \text{Aut}(\mathcal{D}_n^k)$.

**Definition**

For $v \in \mathbb{F}_2^n$, $\sigma \in S_n$, $A_\sigma(v)$ denotes the $n \times n$ matrix with rows $r_i = v + e_{i\sigma}$, for $1 \leq i \leq n$.

E.g. $n = 5$, $\sigma = id$, $v = (1, 1, 0, 0, 0)$, $u = (1, 1, 1, 0, 0)$:

$$A_{id}(v) = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1
\end{bmatrix} \quad \text{and} \quad A_{id}(u) = \begin{bmatrix}
0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1
\end{bmatrix}$$
**Lemma ([FKMd])**

For \( \nu \in \mathbb{F}_2^n, \sigma \in S_n \):

- If \( \nu \) has even weight then \( A_\sigma(\nu) \) is invertible.
- If \( \nu \) has odd weight then \( A_\sigma(\nu) \) is singular.
- If \( \nu \) is even then \( A_\sigma(\nu) \in \text{Aut}(D_n^k) \) for all \( k \geq 1 \) and \( xA_\sigma(\nu) = x\sigma \) for \( x \) even, \( xA_\sigma(\nu) = \nu + x\sigma \) for \( x \) odd.
- If \( k \) is odd and \( \nu \neq 0 \), then \( A_\sigma(\nu) \notin \text{Aut}(\Gamma_n^k) \) for \( n > 2k \), so that \( \text{Aut}(\Gamma_n^k) < \text{Aut}(D_n^k) \).
Proof: Let $V_n = \mathbb{F}_2^n$. If $x = (x_1, \ldots, x_n) \in V_n$, then $xA_{\sigma}(v) = \sum_{i=1}^n x_i(v + e_i\sigma) = (\sum_{i=1}^n x_i)v + x\sigma$.

So $xA_{\sigma}(v) = x\sigma$ if $x$ has even weight, and $xA_{\sigma}(v) = v + x\sigma$ if $x$ has odd weight.

To show $A_{\sigma}(v) \in \text{Aut}(D^1_n)$:

if $x$ and $y$ are on a block of $D^1_n$, then $\text{wt}(x + y) = 2$, and $x, y$ are both even or both odd.

If $x, y$ are even, then $xA_{\sigma}(v) = x\sigma$ and $yA_{\sigma}(v) = y\sigma$, so $xA_{\sigma}(v) + yA_{\sigma}(v) = x\sigma + y\sigma = (x + y)\sigma$, of weight 2.

If $x, y$ are odd then $xA_{\sigma}(v) = v + x\sigma$ and $yA_{\sigma}(v) = v + y\sigma$, so $xA_{\sigma}(v) + yA_{\sigma}(v) = (x + y)\sigma$, of weight 2.

This shows that $A_{\sigma}(v) \in \text{Aut}(D^1_n)$, and hence in $\text{Aut}(D^k_n)$. 
If $k$ is odd, take $\text{wt}(v) = 2m > 0$. Neighbours of 0 are $e$ where $\text{wt}(e) = k$, and have odd weight $k$. So $0A_\sigma(v) = 0$ and $eA_\sigma(v) = v + e\sigma$.

If $A_\sigma(v) \in \text{Aut}(\Gamma^k_n)$ then $\text{wt}(v + e\sigma) = k$ for every $e$ of weight $k$, i.e. $2m = 2\text{wt}(v \cap e\sigma)$ for every $e$ of weight $k$, since $\text{wt}(v + e\sigma) = \text{wt}(v) + \text{wt}(e\sigma) - 2\text{wt}(v \cap e\sigma)$. Thus $m = \text{wt}(v \cap e\sigma) \leq k < n/2$, so $2m < n$. If $S = \text{Supp}(v)$, let $\mathcal{T} = \mathcal{P} \setminus S$, so that $|\mathcal{T}| = n - 2m > 0$. If $n - 2m < k$ then since every weight-$k$ vector must meet $S$ in $m$ points, then any weight-$k$ whose support contains $\mathcal{T}$ must give $k = n - 2m + m$ so that $k + m = n$. This is not possible since $k + m < n/2 + n/2$. If $n - 2m \geq k$ then any weight-$k$ vector in $\mathcal{T}$ does not meet $S$ at all, so we again have a contradiction. Thus $A_\sigma(v) \notin \text{Aut}(\Gamma^k_n)$. ■
Codes from adjacency matrices for $H(n, m)$

- $A_n$ an adjacency matrix for $H(n, m)$, $A_n^* = A_n + I_{m^n}$;
- $D_n(m)$ the neighbourhood $1 - (m^n, (m - 1)n, (m - 1)n)$ symmetric design;
- $C_p(A_n) = C_p(H(n, m)) = C_p(D_n(m))$.
- $D_n^*(m) = 1 - (m^n, (m - 1)n + 1, (m - 1)n)$ design from $A_n^*$.
- $C_p(A_n^*) = C_p(D_n^*(m))$.
- For all $p$, $\dim(C_p(H(n, m)))$ is known: see Peeters [Pee02].

Not a great deal else seems to be known about the codes except for some specific classes (e.g. $Q_n = H(n, 2)$.)
The binary codes of $\mathcal{D}_n(2)$ and $\mathcal{D}_n(2)^*$

$A_n$ an adjacency matrix for $H(n, 2), A_n^* = A_n + I_{2^n}$,
$T$ the translation group of $\mathbb{F}_2^n$,
$T^*$ the group of translations by even-weight vectors of $\mathbb{F}_2^n$.

**Result ([KS07, FKMa])**

- For $n$ odd $A_n$ is invertible.
  For $n$ even $C_2(A_n) = [2^n, 2^{n-1}, n]_2$ self-dual code.
  For $n \geq 6$ even, the minimum words are the rows of $A_n$ and
  $\text{Aut}(C_2(A_n)) = \text{Aut}(\mathcal{D}_n(2)) = (T^* \rtimes S_n) \wr S_2$.

- For $n$ even $A_n + I_{2^n}$ is invertible.
  For $n \geq 5$ odd, $C_2(A_n^*) = [2^n, 2^{n-1}, n + 1]_2$ self-dual code, the
  minimum words are the rows of $A_n^*$, and
  $\text{Aut}(C_2(A_n^*)) = T \rtimes G$, where $G \subseteq \text{GL}_n(\mathbb{F}_2), G \cong S_{n+1}$. 
\[ \text{Aut}(\mathcal{D}_n(2)^*)[FKMb] \]

For \( n \geq 3 \), \( \text{Aut}(\mathcal{D}_n(2)^*) \cong T \rtimes S_{n+1} \) and is primitive for \( n \) even, imprimitive for \( n \) odd;

for \( n \geq 5, \ n \) odd, \( \text{Aut}(C_2(\mathcal{D}_n(2)^*)) = \text{Aut}(\mathcal{D}_n(2)^*) \).
The binary codes of $\mathcal{D}_n(3)$ and $\mathcal{D}_n(3)^*$

$A_n$ an adjacency matrix for $H(n, 3)$, $A_n^* = A_n + I_{2^n}$

$\mathcal{D}_n(3)$ is a symmetric 1-$(3^n, 2n, 2n)$ design from $A_n$;
$\mathcal{D}_n(3)^*$ is a symmetric 1-$(3^n, 2n + 1, 2n + 1)$ design from $A_n^*$.

**Result ([FKM09a])**

If $n \geq 4$, then

- $C = C_2(\mathcal{D}_n(3))$ is $[3^n, \frac{1}{2}(3^n - (-1)^n), 2n]_2$;
- $C^* = C_{\perp} = C_2(\mathcal{D}_n(3)^*)$ is $[3^n, \frac{1}{2}(3^n + (-1)^n), 2n + 1]_2$;

the minimum words of $C$ are the incidence vectors of the blocks of $\mathcal{D}_n(3)$ so

\[
\text{Aut}(C_2(\mathcal{D}_n(3))) = \text{Aut}(\mathcal{D}_n(3)) = \text{Aut}(H(n, 3)) \cong S_3 \wr S_n;
\]

- $C \cap C_{\perp} = \{0\}$
References


W. Fish, J. D. Key, and E. Mwambene.
Codes from the incidence matrices and line graphs of Hamming graphs.

*Discrete Math.* (To appear).

W. Fish, J. D. Key, and E. Mwambene.
Codes from the incidence matrices and line graphs of Hamming graphs \( H^k(n, 2) \) for \( k \geq 2 \).
In preparation.

W. Fish, J. D. Key, and E. Mwambene.
Codes, designs and groups from the Hamming graphs.

W. Fish, J. D. Key, and E. Mwambene.
Graphs, designs and codes related to the \( n \)-cube.

Dina Ghinelli, Marialuisa J. de Resmini, and Jennifer D. Key.
Minimum words of codes from affine planes.
J. D. Key, J. Moori, and B. G. Rodrigues.
Codes associated with triangular graphs, and permutation decoding.

J. D. Key and B. G. Rodrigues.
Codes associated with lattice graphs, and permutation decoding.
Submitted.

J. D. Key and B. G. Rodrigues.
Codes from incidence matrices of strongly regular graphs.
In preparation.

J. D. Key and P. Seneviratne.
Permutation decoding for binary self-dual codes from the graph $Q_n$ where $n$ is even.
On the code generated by the incidence matrix of points and hyperplanes in $PG(n, q)$ and its dual.

On the code generated by the incidence matrix of points and $k$-spaces in $PG(n, q)$ and its dual.

René Peeters.
On the $p$-ranks of the adjacency matrices of distance-regular graphs.

Hassler Whitney.
Congruent graphs and the connectivity of graphs.