Symmetry of Error-Correcting Codes
Entry Faithful 2-Neighbour Transitive Codes

Daniel R. Hawtin

The University of Western Australia

10th December, 2014
Hamming Graphs

Hamming Graph - $\Gamma = H(m, q)$

- Alphabet - set $Q$ ($|Q| = q$)
- Entries - set $M$ ($|M| = m$)
Hamming Graph - $\Gamma = H(m, q)$

- Alphabet - set $Q$ ($|Q| = q$)
- Entries - set $M$ ($|M| = m$)
- Vertex set - strings of length $m$
- Edge set - pairs of strings which differ in one entry
- Distance - $d(\alpha, \beta)$ length of shortest path from $\alpha$ to $\beta$
Hamming Graph - $\Gamma = H(m, q)$
- Alphabet - set $Q$ ($|Q| = q$)
- Entries - set $M$ ($|M| = m$)
- Vertex set - strings of length $m$
- Edge set - pairs of strings which differ in one entry
- Distance - $d(\alpha, \beta)$ length of shortest path from $\alpha$ to $\beta$

$\text{Aut}(\Gamma) = \text{Sym}(Q)^m \rtimes \text{Sym}(M)$
A code $C$ is a subset of the vertices of a graph $H(m, q)$. The minimum distance $\delta = \min \{ d(\alpha, \beta) | \alpha, \beta \in C, \alpha \neq \beta \}$, the covering radius $\rho = \max \{ d(\nu, C) | \nu \in H(m, q) \}$, and the error correction $e = \lfloor \delta - 1 \rfloor$. The automorphism group $\text{Aut}(C) = \text{Aut}(\Gamma)$.
A code $C$ is a subset of the vertices of a graph.

- **minimum distance** $\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$

The diagram illustrates a Hamming graph $H(m, q)$ with a code $C$ and the minimum distance $\delta$. The vertices $\alpha$ and $\beta$ are connected by an edge of length $\delta$. The covering radius $\rho$ is represented by the distance from $\nu$ to the code $C$.
A code \( C \) is a subset of the vertices of a graph.

- **minimum distance** \( \delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\} \)
- \( d(\nu, C) = \min\{d(\nu, \alpha) \mid \alpha \in C\} \)
- **covering radius** \( \rho = \max\{d(\nu, C) \mid \nu \in H(m, q)\} \)
A code $C$ is a subset of the vertices of a graph

- **Minimum distance** $\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$
- $d(\nu, C) = \min\{d(\nu, \alpha) \mid \alpha \in C\}$
- **Covering radius** $\rho = \max\{d(\nu, C) \mid \nu \in H(m, q)\}$
- **Error correction** $e = \left\lfloor \frac{\delta - 1}{2} \right\rfloor$
A code $C$ is a subset of the vertices of a graph

- **minimum distance** $\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$
- $d(\nu, C) = \min\{d(\nu, \alpha) \mid \alpha \in C\}$
- **covering radius** $\rho = \max\{d(\nu, C) \mid \nu \in H(m, q)\}$
- **error correction** $e = \left\lfloor \frac{\delta - 1}{2} \right\rfloor$

Aut($C$) = Aut($\Gamma$)$_C$
Perfect codes - balls of radius \( e \) partition \( H(m, q) \) e.g.
- repetition codes
- Hamming codes
- Golay code

Nearly perfect codes - Goethals (1972) - satisfy Johnson bound e.g.
- Preparata codes

Completely regular codes - Delsarte (1973) - generalise nearly perfect codes e.g.
- Hadamard 12 code
- extended Hamming codes
- extended Preparata codes
Distance Partition

$C_r$ consists of vertices that are distance $r$ from $C$

- $C_r$ is the set of $r$-neighbours

The distance partition:
Any vertex in $C_i$ is adjacent to:

- $a_i$ vertices in $C_i$
- $b_i$ vertices in $C_{i+1}$
- $c_i$ vertices in $C_{i-1}$

$$H(m, q)$$
Completely Regular Codes

Any vertex in $C_i$ is adjacent to:

- $a_i$ vertices in $C_i$
- $b_i$ vertices in $C_{i+1}$
- $c_i$ vertices in $C_{i-1}$

No CR codes known with $\delta > 8$ (except repetition)
Coset-completely transitive codes - (linear) - Solé (1987)
Completely transitive codes - Giudici and Praeger (2000)
Coset-completely transitive codes - (linear) - Solé (1987)

Completely transitive codes - Giudici and Praeger (2000)

- Take $X \leq \text{Aut}(\Gamma)$
- $C$ is CT if each $C_r$ is an $X$-orbit
Algebraic Symmetry of Codes

Coset-completely transitive codes - (linear) - Solé (1987)
Completely transitive codes - Giudici and Praeger (2000)

- Take $X \leq \text{Aut}(\Gamma)$
- $C$ is CT if each $C_r$ is an $X$-orbit

Many codes which are CR are CT, but not all.
Neighbour transitive codes

- Gillespie and Praeger (2011)
- NT if $C$ and $C_1$ are $X$-orbits

$H(m, q)$

$X$ transitive on $C$

$X$ transitive on $C_1$

$C_2$

$\cdots$

$C_\rho$
Neighbour transitive codes

- Gillespie and Praeger (2011)
- NT if $C$ and $C_1$ are $X$-orbits

Found examples, but a classification would be hard.
2-neighbour transitive codes

- My project!
- 2-NT if $C, C_1$ and $C_2$ are $X$-orbits
Example

*Binary repetition code in $H(m, 2)$*

\[
C = \{(0^m), (1^m)\} = \{(0, \ldots, 0), (1, \ldots, 1)\}
\]
Example

Binary repetition code in $H(m, 2)$

$$C = \{(0^m), (1^m)\} = \{(0, \ldots, 0), (1, \ldots, 1)\}$$

- Any permutation in $\text{Sym}(M)$ fixes $C$ setwise
- $h = ((01)^m) = ((01), \ldots, (01))$ swaps $(0^m)$ and $(1^m)$
- $\text{Aut}(C) = 2 \cdot \text{Sym}(M)$
### Definition

We say a group \( X \leq \text{Aut}(C) \) is *entry faithful* if \( X \cong X^M \leq \text{Sym}(M) \)
Entry-Faithful Codes

Definition

We say a group \( X \leq \text{Aut}(C) \) is *entry faithful* if \( X \cong X^M \leq \text{Sym}(M) \)

i.e. if \( 1 \neq h\sigma \in X \) where \( h \in \text{Sym}(Q)^m \) and \( \sigma \in \text{Sym}(M) \)
then \( \sigma \neq 1 \)
Entry Faithful Completely Transitive Codes

- Classified for $|C| \geq 2$ and $\delta \geq 5$ by Gillespie, Giudici and Praeger (2012)
- Only example is the binary repetition code with $X \cong S_m$
Entry Faithful Completely Transitive Codes

- Classified for $|C| \geq 2$ and $\delta \geq 5$ by Gillespie, Giudici and Praeger (2012)
- Only example is the binary repetition code with $X \cong S_m$

Let $h = ((01)^m))$

If $\sigma \in \text{Alt}(M)$ then $\sigma \in X$. Otherwise $h\sigma \in X$. 
A 2-Neighbour Transitive Code

The punctured Hadamard 12 code $\mathcal{P}$ is CT ($\rho = 3$)
The even weight subcode of $\mathcal{P}$ is 2-NT ($\rho = 5$)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
A 2-Neighbour Transitive Code

The punctured Hadamard 12 code $\mathcal{P}$ is CT ($\rho = 3$)
The even weight subcode of $\mathcal{P}$ is 2-NT ($\rho = 5$)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
A 2-Neighbour Transitive Code

The punctured Hadamard 12 code $P$ is CT ($\rho = 3$)
The even weight subcode of $P$ is 2-NT ($\rho = 5$)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
A 2-Neighbour Transitive Code

The punctured Hadamard 12 code $P$ is CT ($\rho = 3$)
The even weight subcode of $P$ is 2-NT ($\rho = 5$)

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1 0 1 1 1 0 0 0 1 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 1 1 0 1 1 1 0 0 0 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0 1 1 0 1 1 1 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 1 0 1 1 0 1 1 1 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0 1 0 1 1 0 1 1 1 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0 0 1 0 1 1 0 1 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0 0 0 1 0 1 1 0 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 0 0 0 1 0 1 1 0 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 1 0 0 0 1 0 1 1 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 1 1 1 0 0 0 1 0 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 0 1 1 1 0 0 0 1 0 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0 0 0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2-neighbour transitive, but not 3-neighbour transitive
Theorem (Gillespie, DH, Giudici, Praeger)

Let $C$ be an $X$ entry faithful 2-neighbour transitive code with $|C| \geq 2$ and $\delta \geq 5$. Then,

- $C$ is the binary repetition code and $X \cong S_m, M_{22} \rtimes 2, X \leq A\Gamma L_d(r)$, or $X \supset PSL_d(r)$; or
- $C$ is the even weight subcode of the punctured Hadamard 12 code and $X \cong M_{11}$. 
Proof Idea

**Theorem (Gillespie, Giudici and Praeger)**

Let $C$ be $EF(X, 2)$-NT. Then $X$ has a 2-transitive action on $M$ and $X_1$ has a 2-transitive action on $Q$. Moreover, $X_0$ has a 2-homogeneous action.
Proof Idea

**Theorem (Gillespie, Giudici and Praeger)**

Let $C$ be $EF (X, 2)$-NT. Then $X$ has a 2-transitive action on $M$ and $X_1$ has a 2-transitive action on $Q$. Moreover, $X_0$ has a 2-homogeneous action.

Consider the socles of $X$ and $X_0$
Proof Idea

Theorem (Gillespie, Giudici and Praeger)

Let \( C \) be EF \((X, 2)\)-NT. Then \( X \) has a 2-transitive action on \( M \) and \( X_1 \) has a 2-transitive action on \( Q \). Moreover, \( X_0 \) has a 2-homogeneous action.

Consider the socles of \( X \) and \( X_0 \)

- equal \( \Rightarrow \) repetition
Proof Idea

**Theorem (Gillespie, Giudici and Praeger)**

Let $C$ be EF $(X, 2)$-NT. Then $X$ has a 2-transitive action on $M$ and $X_1$ has a 2-transitive action on $Q$. Moreover, $X_0$ has a 2-homogeneous action.

Consider the socles of $X$ and $X_0$

- equal $\Rightarrow$ repetition
- $\text{soc}(X) = A_m \Rightarrow$ repetition
Proof Idea

**Theorem (Gillespie, Giudici and Praeger)**

Let $C$ be $EF (X, 2)$-NT. Then $X$ has a 2-transitive action on $M$ and $X_1$ has a 2-transitive action on $Q$. Moreover, $X_0$ has a 2-homogeneous action.

Consider the socles of $X$ and $X_0$

- equal $\Rightarrow$ repetition
- $\text{soc}(X) = A_m \Rightarrow$ repetition
- otherwise $\Rightarrow$ repetition or e.w.p. Hadamard
I would like to thank the Australian Mathematical Society for support to attend this conference.