2-Neighbour Transitive Codes

Daniel R. Hawtin

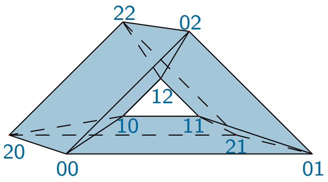
The University of Western Australia

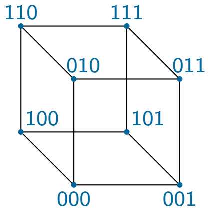
September 27, 2016

Hamming Graphs

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 α to β

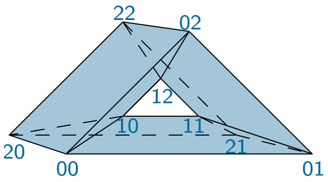


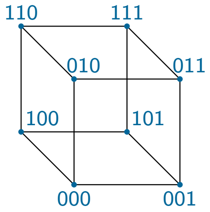


Hamming Graphs

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 α to β

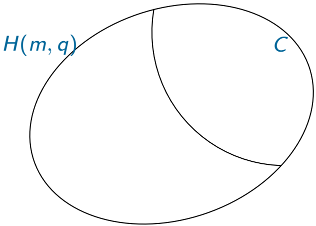




$$\mathrm{Aut}(\Gamma) = \mathrm{Sym}(Q)^m \rtimes \mathrm{Sym}(M)$$

Codes in Hamming Graphs

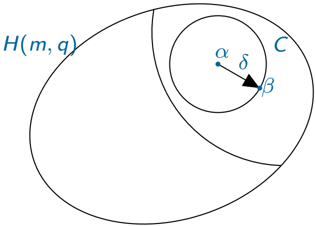
A *code* C is a subset of the vertices of a graph



Codes in Hamming Graphs

A *code* C is a subset of the vertices of a graph

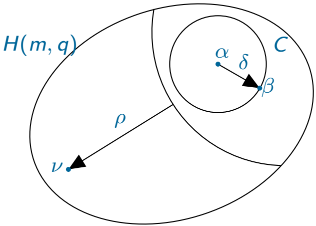
- *minimum distance* $\delta = \min\{d(\alpha,\beta) \mid \alpha,\beta \in C, \alpha \neq \beta\}$



Codes in Hamming Graphs

A *code* C is a subset of the vertices of a graph

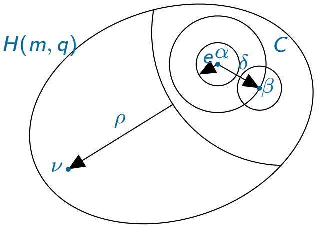
- *minimum distance* $\delta = \min\{d(\alpha, \beta) \mid \alpha, \beta \in C, \alpha \neq \beta\}$
- $d(\nu, C) = \min\{d(\nu, \alpha) \mid \alpha \in C\}$
- *covering radius* $\rho = \max\{d(\nu, C) \mid \nu \in H(m, q)\}$



Codes in Hamming Graphs

A *code* C is a subset of the vertices of a graph

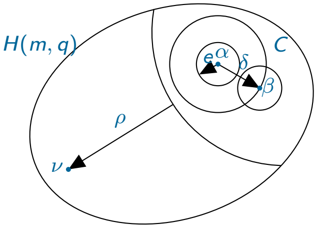
- *minimum distance* $\delta = \min\{d(\alpha,\beta) \mid \alpha,\beta \in C, \alpha \neq \beta\}$
- $d(\nu, C) = \min\{d(\nu,\alpha) \mid \alpha \in C\}$
- *covering radius* $\rho = \max\{d(\nu, C) \mid \nu \in H(m,q)\}$
- *error correction* $e = \left\lfloor \frac{\delta-1}{2} \right\rfloor$



Codes in Hamming Graphs

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* $e = \left\lfloor \frac{\delta - 1}{2} \right\rfloor$

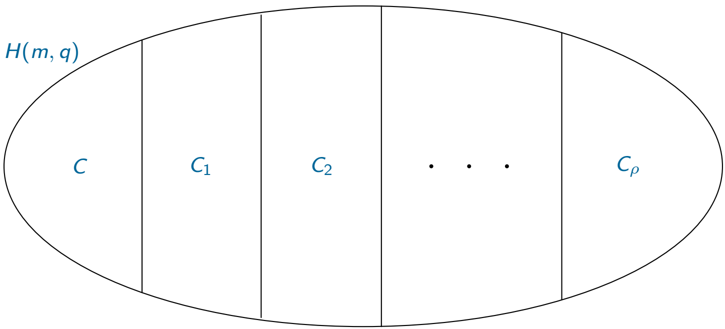


$$\mathrm{Aut}(C) = \mathrm{Aut}(\Gamma)_C$$

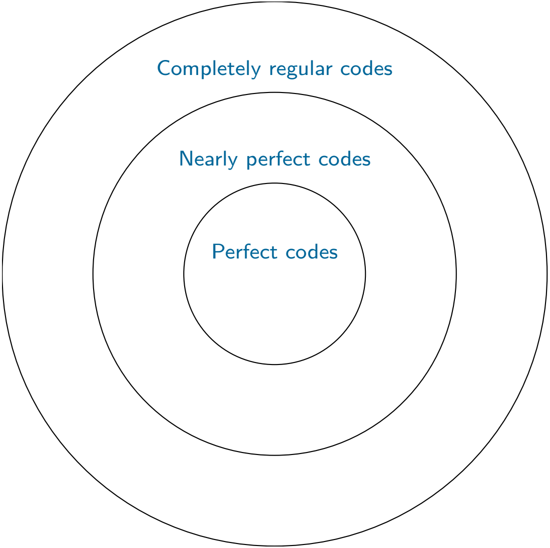
Distance Partition

Define the *set of s-neighbours* C_s to be all vertices $\alpha \in H(m, q)$ with $d(\alpha, C) = s$

The *distance partition*:



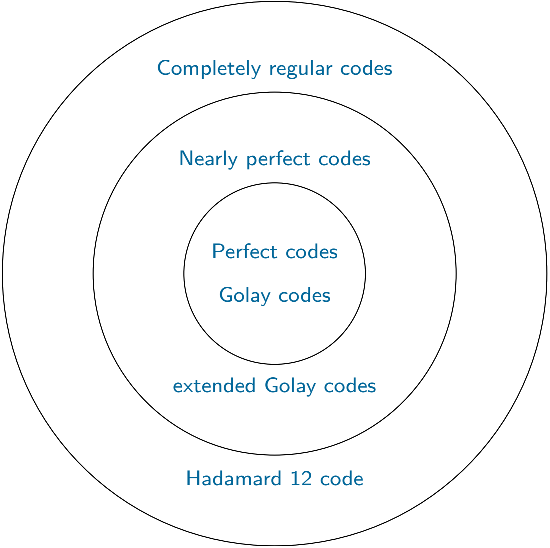
Combinatorial Symmetry of Codes



Delsarte (1973)

Goethals (1972)

Combinatorial Symmetry of Codes

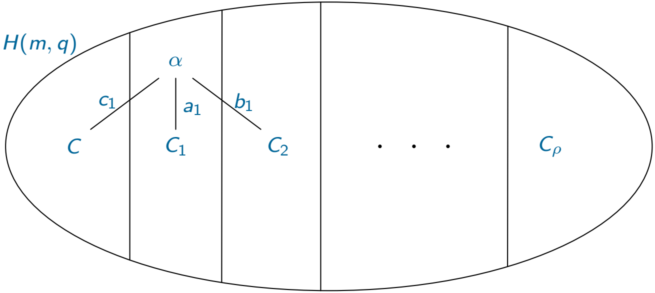


Delsarte (1973)

Goethals (1972)

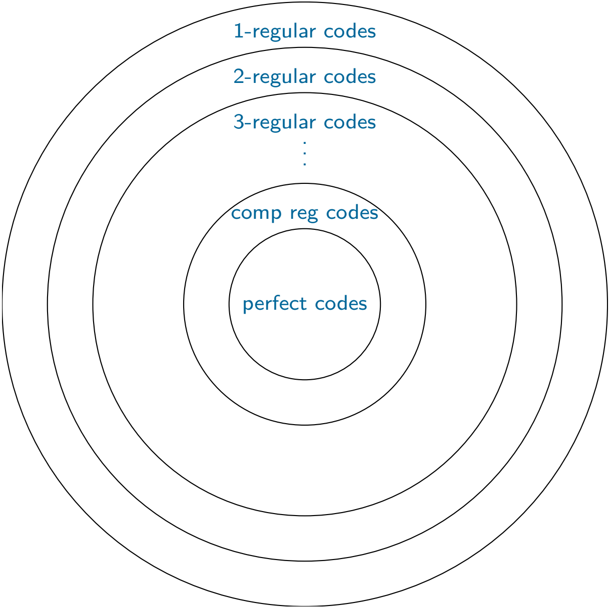
Completely Regular Codes

Completely regular - for any $i \in \{0, 1, \ldots, \rho\}$, any two vertices in C_i are adjacent to the same number of vertices from each of C_{i-1}, C_i and C_{i+1}



C is *s-regular* if this holds for each $i \in \{0, 1, \ldots, s\}$, for some $s \leqslant \rho$

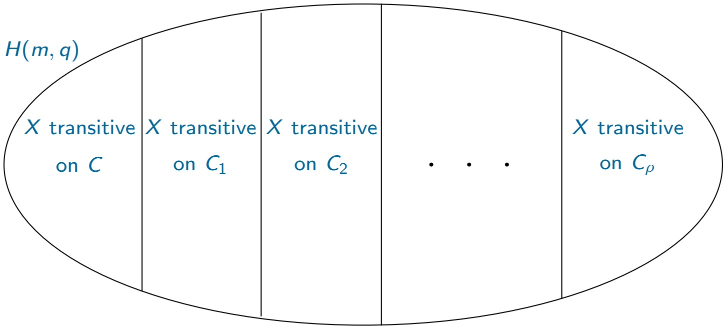
Combinatorial Symmetry of Codes



Algebraic Symmetry of Codes

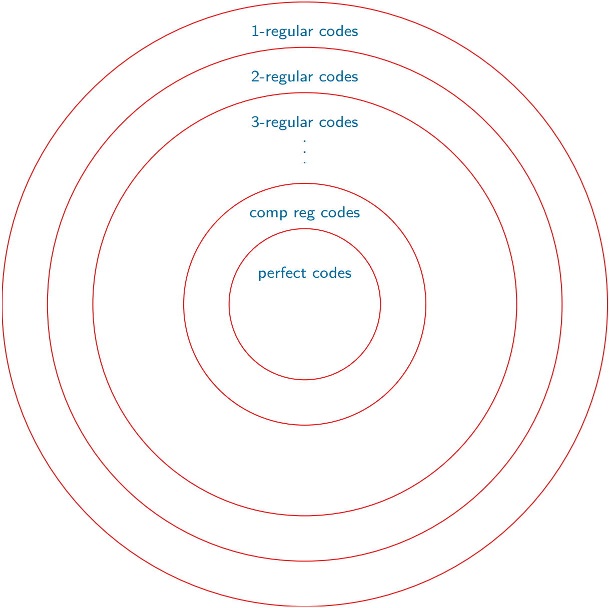
Solé (1987), refined by Giudici and Praeger (2000)

$\exists\ X \leqslant \mathrm{Aut}(C)$ s.t. C_i is an X-orbit for $i \in \{0, 1, \ldots, \rho\}$

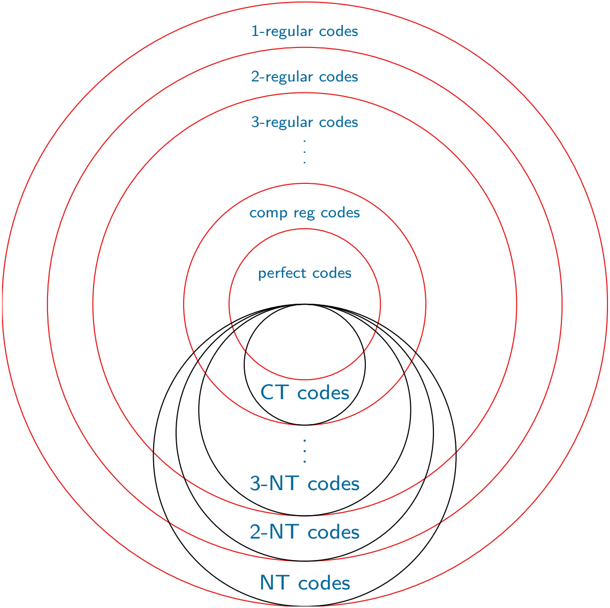


C is *s-neighbour transitive* if this instead holds for each $i \in \{0, 1, \ldots, s\}$, for some $s \leqslant \rho$ - Gillespie and Praeger (2011)

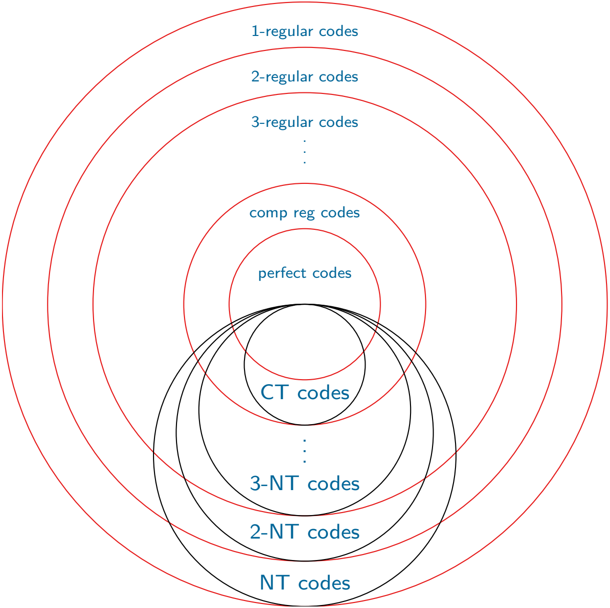
Algebraic Symmetry of Codes



Algebraic Symmetry of Codes

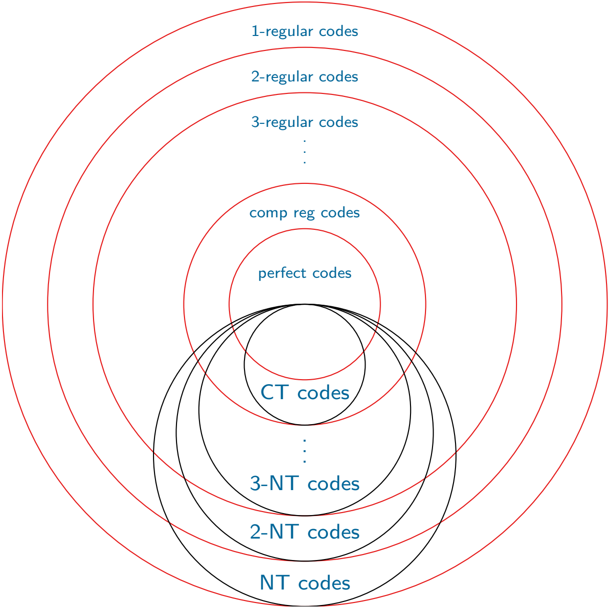


Algebraic Symmetry of Codes



Examples

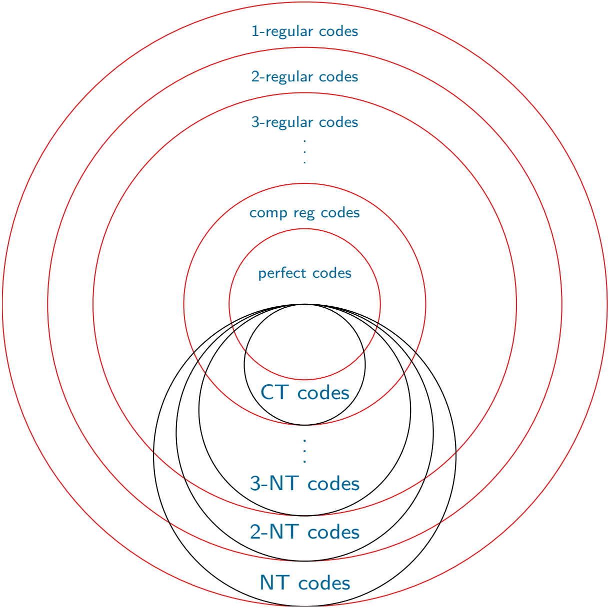
Algebraic Symmetry of Codes



Examples

Preparata codes

Algebraic Symmetry of Codes

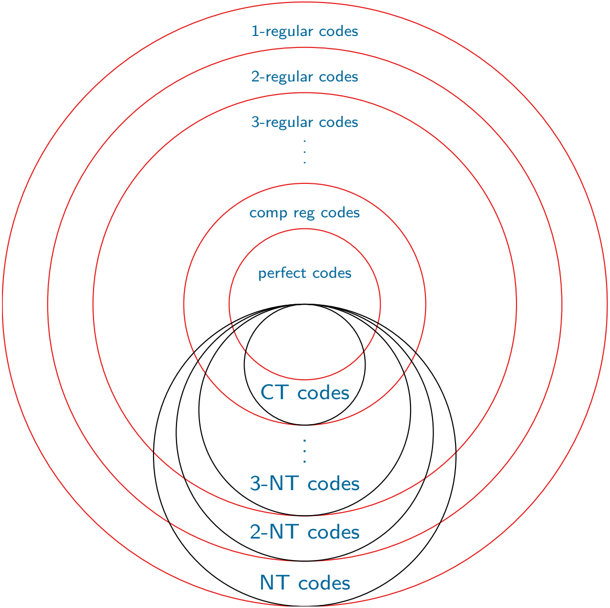


Examples

Preparata codes

Hamming-like codes

Algebraic Symmetry of Codes



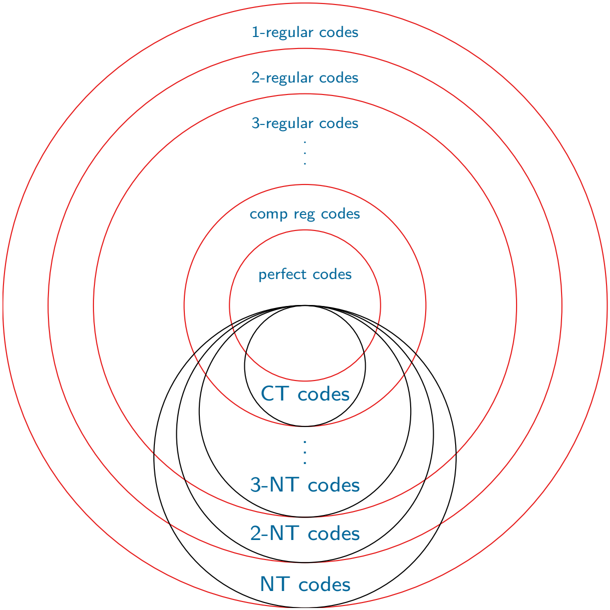
Examples

Preparata codes

Hamming-like codes

extended Golay codes

Algebraic Symmetry of Codes



Examples

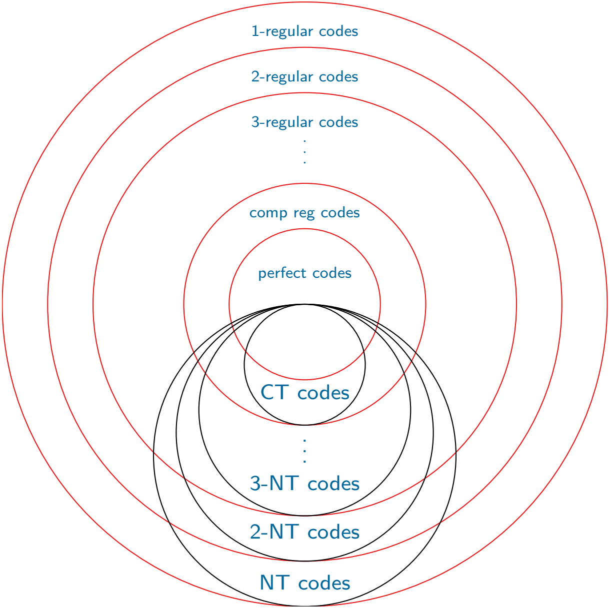
Preparata codes

Hamming-like codes

extended Golay codes

projective Reed-Muller codes

Algebraic Symmetry of Codes



Examples

Preparata codes

Hamming-like codes

extended Golay codes

projective Reed-Muller codes

permutation codes

Reed-Muller codes

Reed-Muller codes:

- vertices - $\{f : \mathbb{F}_q^d \to \mathbb{F}_q\}$
- $M = \mathbb{F}_q^d$
- $Q = \mathbb{F}_q$
- $\mathrm{GL}_d(q)$ acts as 'pure permutations'
- $f^g(x) = f(x^{g^{-1}})$
- $\mathrm{GL}_d(q)$ is 2-transitive on entries
- codes are subspaces defined by the degree of the poly. representing the vertices
- only *guarenteed* to be neighbour transitive

Projective Reed-Muller codes:

- vertices - $\{f : \mathbb{F}_q^d \to \mathbb{F}_q \mid f(ax) = af(x)\}$
- $M =$ 1-dim subspaces of $\mathbb{F}_q^d$
- $Q =$ set of linear fns $\mathbb{F}_q \to \mathbb{F}_q$
- $\mathrm{GL}_d(q)$ acts, but *not* as 'pure permutations'
- $f^g(x) = f(x^{g^{-1}})$
- $\mathrm{GL}_d(q)$ is 2-transitive on weight two vectors
- codes are subspaces defined by the degree of the poly. representing the vertices
- at least 2-neighbour transitive

Suzuki, Ree and Unitary Groups

Codes similar to proj. Reed-Muller with $X_{\mathbf{0}}^M \cong \mathrm{Sz}(q)$, $\mathrm{Ree}(q)$ or $\mathrm{PSU}_3(q)$:

- vertices - $\{f : \mathbb{F}_q^d \to \mathbb{F}_q \mid f(ax) = af(x)\}$
- $M =$ some set of 1-dim subspaces of $\mathbb{F}_q^d$ (inversive plane, Ree unital, isotropic subspaces)
- $Q =$ set of linear fns $\mathbb{F}_q \to \mathbb{F}_q$
- $f^g(x) = f(x^{g^{-1}})$
- $X_{\mathbf{0}}$ is 2-transitive on weight two vectors
- codes defined similarly to PRM
- at least 2-neighbour transitive

Suzuki, Ree and Unitary Groups

Codes similar to proj. Reed-Muller with $X_{\mathbf{0}}^{M} \cong \mathrm{Sz}(q)$, $\mathrm{Ree}(q)$ or $\mathrm{PSU}_3(q)$:

- vertices - $\{f : \mathbb{F}_q^d \to \mathbb{F}_q \mid f(ax) = af(x)\}$
- $M =$ some set of 1-dim subspaces of $\mathbb{F}_q^d$ (inversive plane, Ree unital, isotropic subspaces)
- $Q =$ set of linear fns $\mathbb{F}_q \to \mathbb{F}_q$
- $f^g(x) = f(x^{g^{-1}})$
- $X_{\mathbf{0}}$ is 2-transitive on weight two vectors
- codes defined similarly to PRM
- at least 2-neighbour transitive
- new codes (afawk)

Action on Entries

Consider the action X^M of X on the set M of entries:

Lemma

Suppose C is 2-neighbour transitive with minimum distacnce $\delta \geq 5$. Then X^M is 2-homogeneous.

Sketch:

- $X_{\mathbf{0}}$ is transitive on weight two vertices (uses $\delta \geq 5$)
- each weight two codeword is non-zero in two entries
- so $X_{\mathbf{0}}^M$ is 2-homogeneous

Action on the Alphabet Q

Consider the subgroup X_1 stabilising $1 \in M$ and its action X_1^Q on Q:

Lemma

Suppose C is 2-neighbour transitive with minimum distacnce $\delta \geq 5$. Then X_1^Q is 2-transitive.

Sketch:

- Weight δ codewords form a (q-ary) 2-design,
- $\exists$ codeword that starts with $a \in Q^*$,
- X transitive $C \Rightarrow X_1^Q$ transitive, (uses $X_{\mathbf{0}}^M$ 2-hom.)

Action on the Alphabet Q

Consider the subgroup X_1 stabilising $1 \in M$ and its action X_1^Q on Q:

Lemma

Suppose C is 2-neighbour transitive with minimum distacnce $\delta \geq 5$. Then X_1^Q is 2-transitive.

Sketch:

- Weight δ codewords form a (q-ary) 2-design,
- $\exists$ codeword that starts with $a \in Q^*$,
- X transitive $C \Rightarrow X_1^Q$ transitive, (uses $X_{\mathbf{0}}^M$ 2-hom.)
- $(X_{\mathbf{0},1})^Q$ transitive on neighbours $\Rightarrow X_1^Q$ 2-transitive.

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 ($\rho = 5$).

0	1	2	3	4	5	6	7	8	9	10
1	1	0	1	1	1	0	0	0	1	0

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 ($\rho = 5$).

0	1	2	3	4	5	6	7	8	9	10
1	1	0	1	1	1	0	0	0	1	0
0	1	1	0	1	1	1	0	0	0	1
1	0	1	1	0	1	1	1	0	0	0
0	1	0	1	1	0	1	1	1	0	0
0	0	1	0	1	1	0	1	1	1	0
0	0	0	1	0	1	1	0	1	1	1
1	0	0	0	1	0	1	1	0	1	1
1	1	0	0	0	1	0	1	1	0	1
1	1	1	0	0	0	1	0	1	1	0
0	1	1	1	0	0	0	1	0	1	1
1	0	1	1	1	0	0	0	1	0	1

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 ($\rho = 5$).

0	1	2	3	4	5	6	7	8	9	10
1	1	0	1	1	1	0	0	0	1	0
0	1	1	0	1	1	1	0	0	0	1
1	0	1	1	0	1	1	1	0	0	0
0	1	0	1	1	0	1	1	1	0	0
0	0	1	0	1	1	0	1	1	1	0
0	0	0	1	0	1	1	0	1	1	1
1	0	0	0	1	0	1	1	0	1	1
1	1	0	0	0	1	0	1	1	0	1
1	1	1	0	0	0	1	0	1	1	0
0	1	1	1	0	0	0	1	0	1	1
1	0	1	1	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0

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 ($\rho = 5$).

0	1	2	3	4	5	6	7	8	9	10
1	1	0	1	1	1	0	0	0	1	0
0	1	1	0	1	1	1	0	0	0	1
1	0	1	1	0	1	1	1	0	0	0
0	1	0	1	1	0	1	1	1	0	0
0	0	1	0	1	1	0	1	1	1	0
0	0	0	1	0	1	1	0	1	1	1
1	0	0	0	1	0	1	1	0	1	1
1	1	0	0	0	1	0	1	1	0	1
1	1	1	0	0	0	1	0	1	1	0
0	1	1	1	0	0	0	1	0	1	1
1	0	1	1	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0

2-neighbour transitive, but not 3-neighbour transitive.

Entry-Faithful (EF) Codes

Entry faithful - kernel of X^M is trivial

C entry-faithful completely transitive with $\delta \geq 5$ implies C is the repetition code (Gillespie, Giudici and Praeger - 2012)

Entry-Faithful (EF) Codes

Entry faithful - kernel of X^M is trivial

C entry-faithful completely transitive with $\delta \geq 5$ implies C is the repetition code (Gillespie, Giudici and Praeger - 2012)

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 $X \cong S_m, M_{22} \rtimes 2$, $X \leqslant \mathrm{A\Gamma L}_d(r)$, or $X \trianglerighteq \mathrm{PSL}_d(r)$; or*
- *C is the even weight subcode of the punctured Hadamard 12 code and $X \cong M_{11}$.*

Alphabet-Almost-Simple Codes

Here the 2-transitive action X_1^Q is almost-simple

Gillespie and Praeger (2012) characterised alphabet-almost-simple (AAS) 1-NT codes with $\delta \geq 3$ by the blocks of imprimitivity of C

Several infinite families of possible blocks are obtained from *permutation codes* - codewords defined by permutations: $\alpha(g) = (1^g, 2^g, \ldots, q^g)$

Alphabet-Almost-Simple Codes

Here the 2-transitive action X_1^Q is almost-simple

Gillespie and Praeger (2012) characterised alphabet-almost-simple (AAS) 1-NT codes with $\delta \geq 3$ by the blocks of imprimitivity of C

Several infinite families of possible blocks are obtained from *permutation codes* - codewords defined by permutations: $\alpha(g) = (1^g, 2^g, \ldots, q^g)$

Theorem (Gillespie, DH)

Let C be an AAS 2-NT code in $H(m, q)$, with $\delta \geq 3$. Then $m = \delta = 3$, $q \geq 5$ and C is equivalent to the repetition code with these parameters.

Alphabet-Affine Codes

Here the 2-transitive action X_1^Q is affine.

First we considered the case where the kernel of the action X^M is a one-dim. vector space

Theorem (Gillespie, DH, Praeger)

Let C be an alphabet-affine 2-NT code in $H(m, q)$, with $\delta \geq 5$, containing a block of imprimitivity which is a 1-dimensional vector space. Then $q = 2$ and C is equivalent to the repetition code, the Hadamard code of length 12 or its punctured code.

Alphabet-Affine Codes

This is the final part of my project. What we know:

- The kernel $K_{\mathbf{0}}$ of the action $X_{\mathbf{0}}^{M}$ can be taken to be a straight diagonal subgroup acting semi-regularly on $Q^{\times}$
- An isomorphic copy of $K_{\mathbf{0}}$ must appear as a normal subgroup of the transitive linear group $X_{\mathbf{0},1}^{Q^{\times}}$
- We have used this to show $K_{\mathbf{0}}$ is soluble
- $X_{\mathbf{0},1,2}^{Q^{\times}}$ is also transitive
- C has a block of imrprimitivity which is a vector space

Alphabet-Affine Codes

This is the final part of my project. What we know:

- The kernel $K_{\mathbf{0}}$ of the action $X_{\mathbf{0}}^{M}$ can be taken to be a straight diagonal subgroup acting semi-regularly on $Q^{\times}$
- An isomorphic copy of $K_{\mathbf{0}}$ must appear as a normal subgroup of the transitive linear group $X_{\mathbf{0},1}^{Q^{\times}}$
- We have used this to show $K_{\mathbf{0}}$ is soluble
- $X_{\mathbf{0},1,2}^{Q^{\times}}$ is also transitive
- C has a block of imrprimitivity which is a vector space

We aim use the interplay between the 2-homogeneous $X_{\mathbf{0}}^{M}$ and the transitive linear groups $X_{\mathbf{0},1}^{Q^{\times}}$ and $X_{\mathbf{0},1,2}^{Q^{\times}}$ to characterise the possible blocks of imprimitivity of C

Elusive codes

For an *s-elusive code*, the group of automorphisms of the s-neighbours is larger than that of the code

Theorem (DH)

Let C be an s-elusive code in $H(m, q)$ with $\delta \geq 2s + 1$. Then there exists a q-ary s-$(m, 2s, 1)$-design.

- certain permutation codes are 1-elusive
- Reed-Muller codes are 1-elusive
- Preparata codes are 2-elusive
- the even weight subcode of the perfect Golay code is 3-elusive

Future directions

Possible future work includes:

- Classify all 2-neighbour transitive codes from blocks
- Explicitly classify all completely transitive codes
- Explore designs from any new codes
- Extend techniques to look ak imprimitive rank 3 groups
- Classify those 2-neighbour transitive codes which are also elusive

Cheers!

Thanks!