THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

Symmetry of codes in graphs

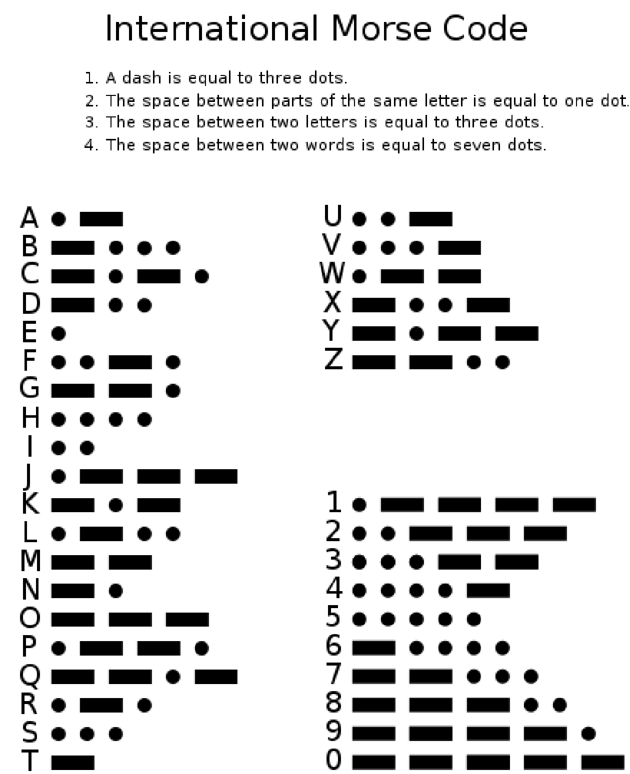
Cheryl E Praeger

Centre for Mathematics of Symmetry and Computation

THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

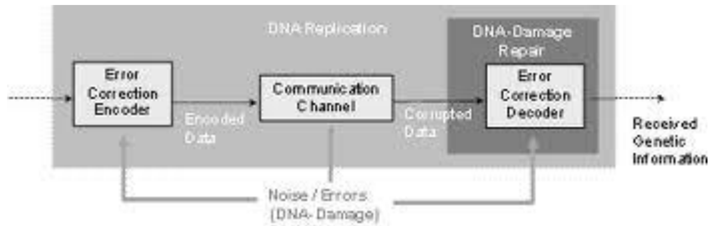
Communicating Information

Electronically brings   danger of introducing errors



THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

Standard representation

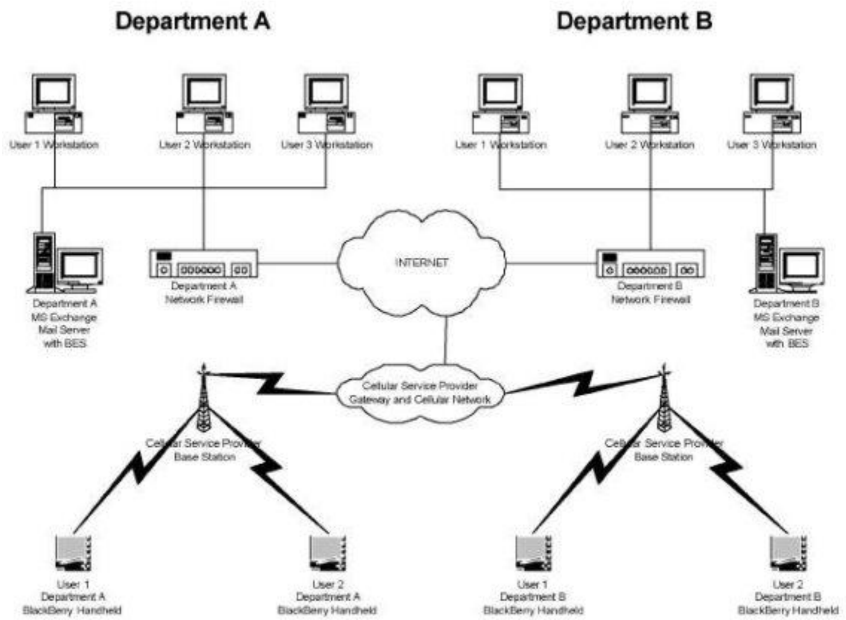


Block codes:

Codewords are strings

Errors are incorrect entries

Distance(sent, received)
= number of errors



Codes in Graphs

1973 Delsarte

•Interpret vertex subsets C of any graph X as codes

•vertices in C are codewords

•Introducing a “single error” into a codeword v gives vertex u at distance 1 from v in X

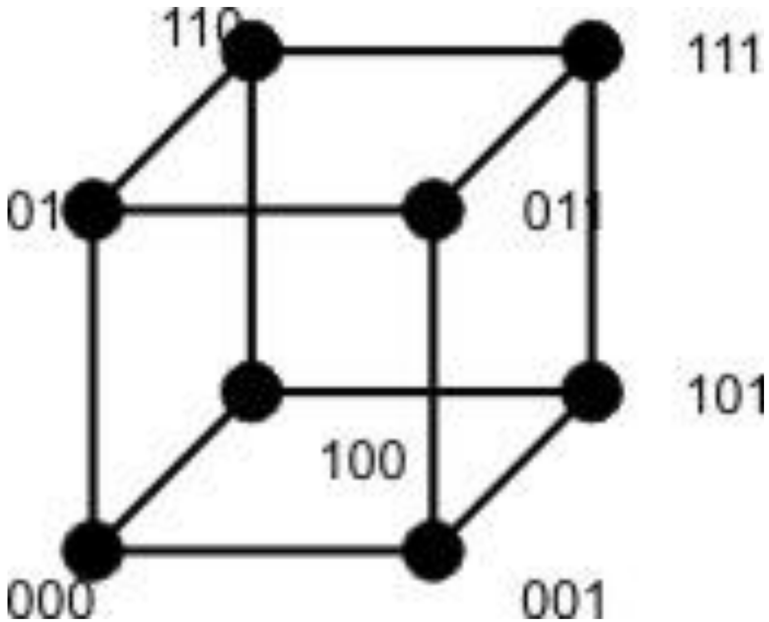
•if u not in C then call u a neighbour of code C

Classical setup:
X = H(m,q) a Hamming graph

In H(3,2) take

C={ 000, 111 } so δ = 3

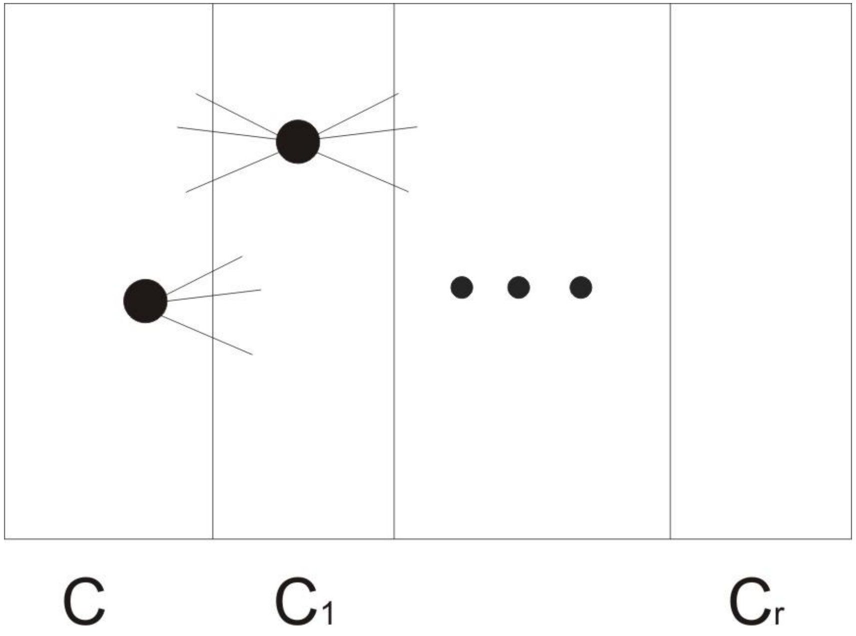
- VX = m-tuples from alphabet of size q
- { x, y } edge in X if x, y differ in one entry
- Distance d(x,y) = number of different entries
- Minimum distance δ for C is least d(x,y) for x,y in C



Delsarte suggested: take X a completely regular graph

The University of Western Australia
Achieve International Excellence

Distance partition of C



C_1 = neighbour set of C
r = covering radius

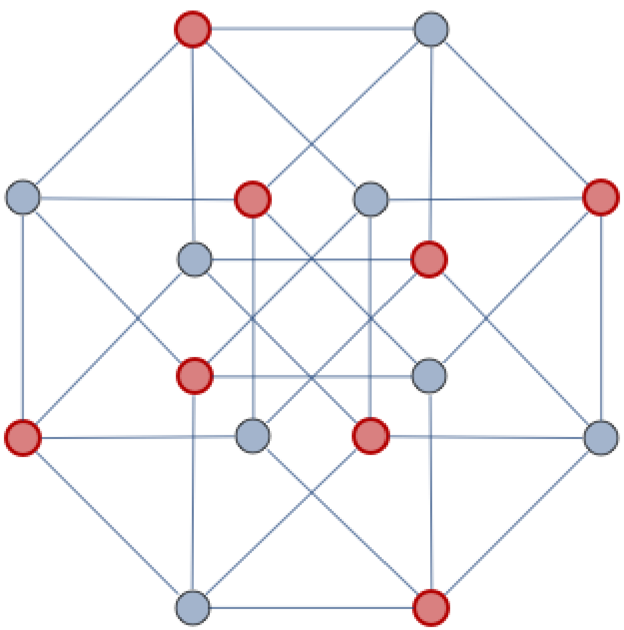
Introduced completely regular codes

- Distance partition is equitable
- For v in C_i numbers of edges from v to vertices in C_j depend only on i and j – independent of v

Example of completely regular code

The University of Western Australia
Achieve International Excellence

C in H (4 , 2)



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Minimum distance $\delta = 2$
covering radius = 1

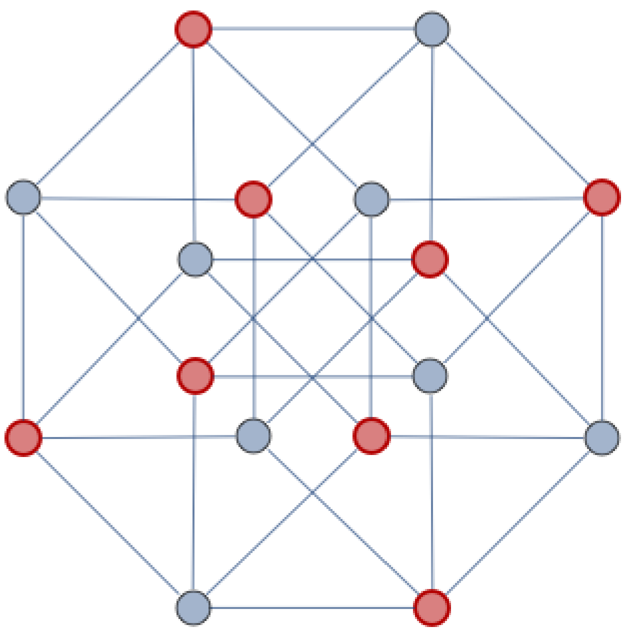
Completely regular codes

- Delsarte: Generalising perfect codes
- Disappointingly not many CR codes known with large minimum distance δ
- Led to Conjectures for CR codes in H(m,q)

THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

Conjectures for CR codes in H(m,q)

C in H (4 , 2)



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

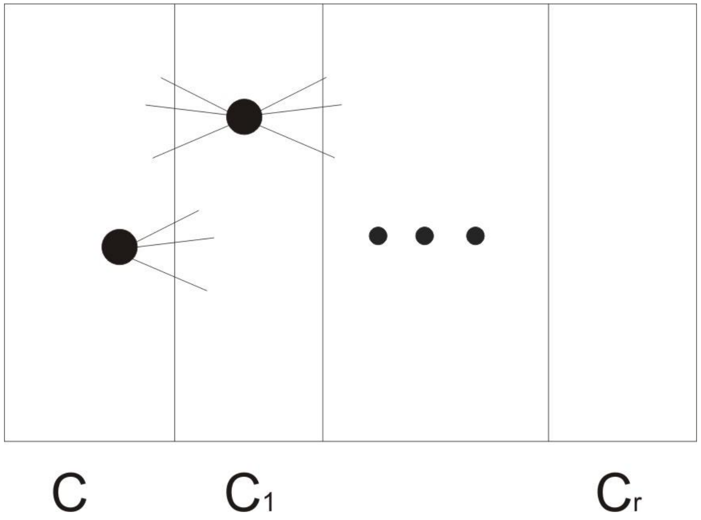
Minimal distance $\delta = 2$
covering radius = 2

Conjectures

- Neumaier 1992 only CR code in an H(m,q) with $\delta = 8$ is the binary Golay code
- Borges, Rifa, Zinoviev 2001 every CR code in an H(m,q) has δ at most 8

Two directions for further study using symmetry

Automorphism group Aut(C):
Setwise stabilser of C in Aut(X)



For all codes C:

- Aut(C) leaves each C_i invariant

C is completely transitive:

- Aut(C) is transitive on C_i for each i

Warning: Some use **more restrictive definition of Aut(C) !!**

Work on completely transitive codes in graphs

In H(m,q)

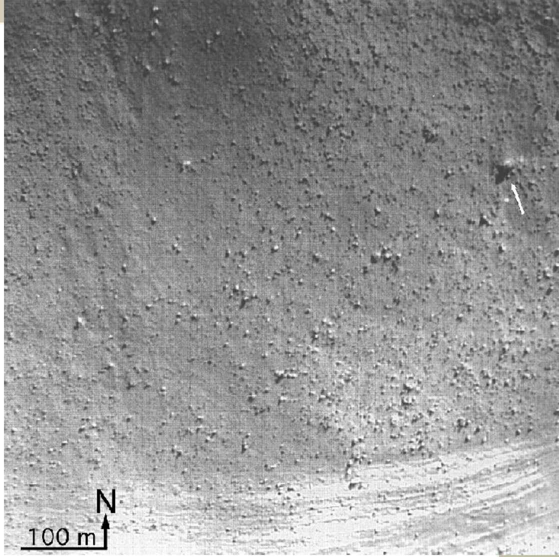
- Patrick Sole
- Michael Giudici and CEP
- Rifa and Zinoviev: with restrictive Aut(C) show δ at most 8
- Neil Gillespie PhD 2012

In Johnson graphs J(v,k)

- Bill Martin
- Chris Godsil and CEP

An example:

NASA *space* probe Mariner 9 in 1971 used the Hadamard code n=32 to transmit *photos* of Mars back to Earth



Hadamard codes

- Take Hadamard matrix H
- “Double and negate”
- Change -1 to 0
- Code(H) in H(n,2)
- Automorphism (P, Q) with H=PHQ with P, Q monomial
- Aut(H) = Aut(Code(H))
- size 2n , $\delta = n/2$

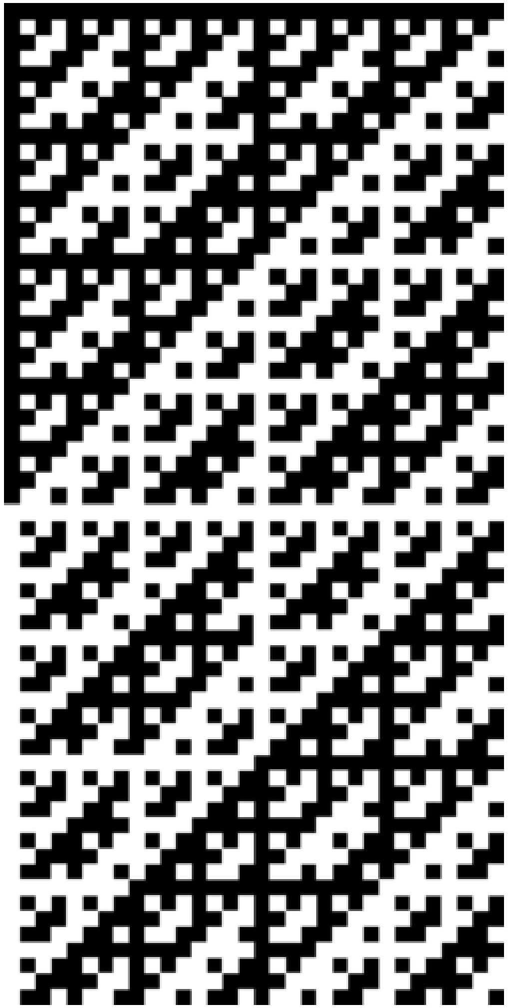
Tiny Example:

$$\begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix} \Rightarrow \begin{matrix} 1 & 1 \\ 1 & -1 \\ -1 & -1 \\ -1 & 1 \end{matrix} \Rightarrow \begin{matrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{matrix}$$

A completely transitive Hadamard code

Neil Gillespie and CEP

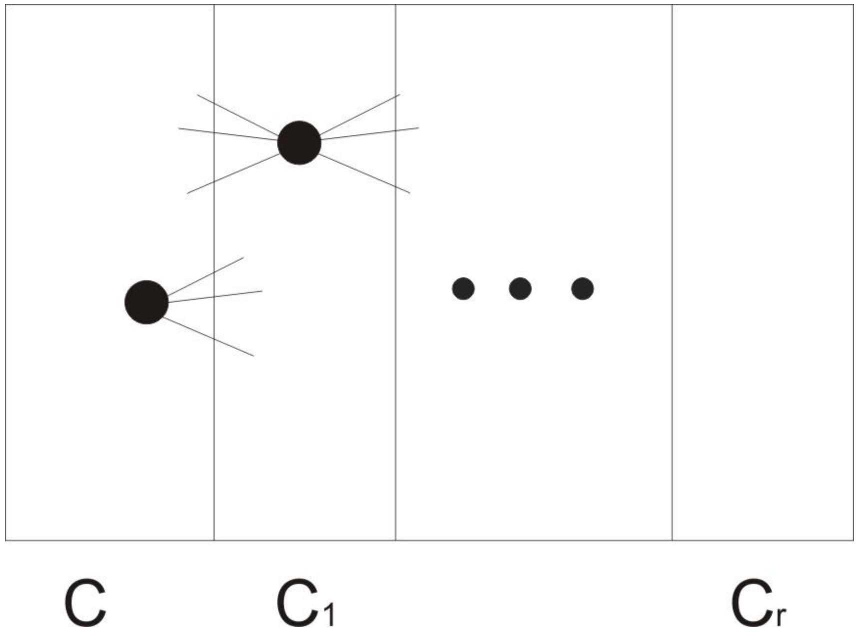
- Unique12 x 12 matrix H
- 1962 M Hall Aut(H)=2.M_{12}
- Code(H) is completely transitive!
- δ = 6
- Covering radius = 3



Second direction: neighbour-transitive codes

Aut(C) transitive on C & C_1

- Gillespie: C in H(m,q)
- Liebler & CEP: C in J(v,k)



We don't care about the "far-away" vertices

Neil Gillespie's work

Constructions & Classifications

- Remarkable new family of codes C(T)
- Building blocks for large class of neighbour-transitive codes

Neil's C(T) codes

Choose favourite permutation group T

- Each x in T becomes a codeword:
- E.g. If $T=S_3$ then (123) sometimes written as

  1 2 3
  2 3 1

- Take associated codeword as (2 3 1) = $(1^x\ 2^x\ 3^x)$

Gillespie & CEP

For $T = S_3$ on { 1, 2, 3 }

- C(T) in H(3,3)
- |T| = 6 codewords
- Length 3, Alphabet {1,2,3}
- Distance between

$(1^x\ 2^x\ 3^x)$ and $(1^y\ 2^y\ 3^y)$

Is number of points moved by xy^{-1} so $\delta = 2$ for $C(S_3)$

In Neil's classification T is simple "socle" of 2-transitive group

- δ = minimal degree(T)
- Aut (C(T)) contains T x T and is neighbour-transitive
- Proof uses 2-transitivity

Gillespie & CEP

T=PSL(2,29) on PG(1,29)

- C(T) in H(30,30)
- Size |T| ≈ 13K
- Length 30 = |PG(1,29)|
- Alphabet PG(1,29)
- δ = 28 = minimal degree(T)
- So corrects 13 errors!

N. Tr. codes in Johnson graphs

Johnson graph J(v,k) **Based on a v-set *V***

Johnson graph $J(v, k)$ based on v-set $\mathcal{V}$

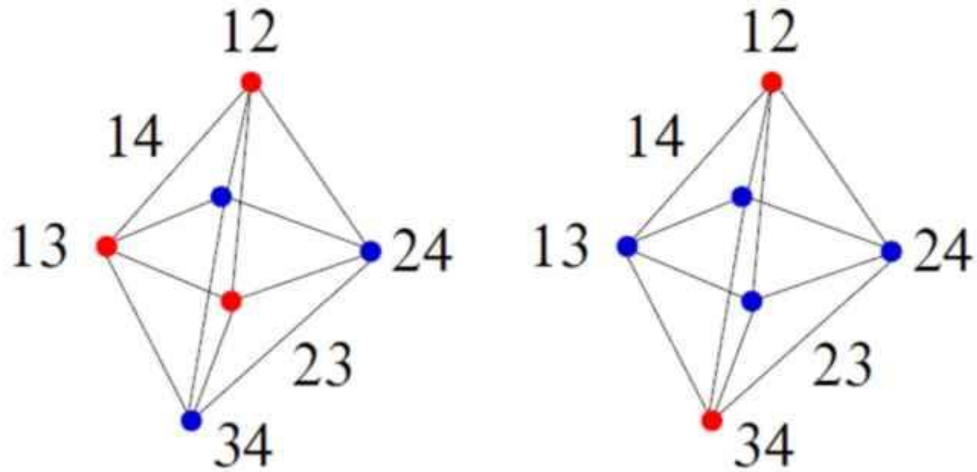
- vertex set $\binom{\mathcal{V}}{k}$
- arc set J: all vertex pairs (α, α_1) with $|\alpha \cap \alpha_1| = k - 1$
- distance in $J(v, k)$: $d_J(\alpha, \beta) = i \Leftrightarrow |\alpha \cap \beta| = k - i$

View code C as subset of vertices of $J(v, k)$

Neighbour set $C_1 = \{\gamma_1 \notin C \mid d_J(\gamma, \gamma_1) = 1 \ \exists\, \gamma \in C\}$
Minimum distance $\delta(C) = $ minimum of $d_J(\gamma, \gamma') = k - |\gamma \cap \gamma'|$
where $\gamma, \gamma' \in C, \gamma \neq \gamma'$

$\mathrm{Aut}(C) < \mathrm{Aut}(J(v,k)) = \mathrm{Sym}(V)=S_v$

THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence



C in J(4,2)

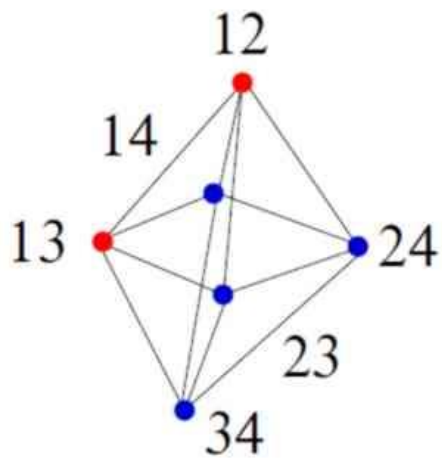
Example 1. $C = \{12, 13, 23\}$, $C_1 = \{14, 24, 34\}$,

$\mathrm{Aut}(C) = S_3 = \langle (12), (123) \rangle$

Example 2. $C = \{12, 34\}$, $C_1 = \{13, 14, 23, 24\}$,
$\mathrm{Aut}(C) = D_8 = \langle (12), (1324) \rangle$

Aut(C) < Aut(J(v,k)) = Sym(V)=S_v

C in J(4,2)



Non-Example 3. $C = \{12, 13\}$, $C_1 = \{14, 22, 24, 34\}$,

$\mathrm{Aut}(C) = \langle (23) \rangle$ transitive on C (code-transitive) but not on C_1

Non-Example 4. $C = \{14, 22, 24, 34\}$, $C_1 = \{12, 13\}$,
$\mathrm{Aut}(C)$ transitive on C_1 but not on C.

Some Questions:

- Are there many examples?
- Are most completely transitive?
- How large can $\delta(C)$ be?
- $\exists$ examples involving interesting ‘geometry’?
- Is any kind of classification feasible?

Comment on “design” interpretation

- Since vertices in J(v,k) are k-sets
- Natural to interpret codes C in J(v,k) as designs
- Nice examples arise from nice designs!

A few nice neighbour-transitive examples

- Blocks of 2-(11, 5, 2) biplane in J(11,5) with group PSL(2,11)
- Blocks of the Witt designs for Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24} and other goodies!
- Quadrics in the Higman-Sims graph with group HS i.e. a 2-(176,50,14) design
- Exactly four examples with group Co_3 and v=276, k = 6, 36, 100, 126

This classification problem comes from a reduction to problem about 2-transitive permutation groups

- Case of sporadic 2-transitive permutation groups (such as Mathieu groups, HS, Co_3)
- Finite problem solved using theory and GAP
- Collaboration with Max Neunhoeffer
- Complete list of sporadic examples [21 of them] along with their minimum distances δ

Comment on "code" interpretation arising from discussions with Max

- Since vertices in J(v,k) are k-sets
- Another natural interpretation: codeword = binary v-tuple [characteristic function of the k-set]
- Then C becomes a constant weight binary code in Hamming graph H(v,2)
- Distance between code words in H(v,2)
  = 2 x distance in J(v,k)
- Group of C in Aut(J(v,k)) contained in group of C in Aut(H(v,2)) – neighbour transitivity does not go through

Comment on “complements”

- Given code C in $J(v, k)$

  for $\gamma \subset \mathcal{V}$ write $\overline{\gamma} = \mathcal{V} \setminus \gamma$
- Define $\overline{C} = \{\overline{\gamma} \mid \gamma \in C\}$ $\quad \overline{C}_1 = \{\overline{\gamma}_1 \mid \gamma_1 \in C_1\}$
- Then $\overline{C}$ is a code in $J(v, v-k) \cong J(v, k)$ with ‘block size’ $v - k$

  $\overline{C}$ has neighbour set $\overline{C}_1$ and $\mathrm{Aut}(C) = \mathrm{Aut}(\overline{C})$

  $\overline{C}$ is neighbour-transitive $\Leftrightarrow$ C is neighbour-transitive

  so assuming $k \leq \frac{v}{2}$ really no restriction

The University of Western Australia
Achieve International Excellence

Comment on “geometrical” interpretation

- Regard (C, C_1) as an incidence structure. For $\gamma \in C, \gamma_1 \in C_1$, (γ, γ_1) incident $\Leftrightarrow d_J(\gamma, \gamma_1) = 1$
  - Let $\textsc{Inc}(C, C_1)$ be set of incident (γ, γ_1) with $\gamma \in C, \gamma_1 \in C_1$
  - C is called incidence-transitive if $\mathrm{Aut}(C)$ is transitive on $\textsc{Inc}(C, C_1)$
- if $\delta(C) \geq 2$, then C incidence-trans $\Rightarrow$ C neighbour-trans
- if $\delta(C) \geq 3$, then C incidence-trans $\Leftrightarrow$ C neighbour-trans

More neighbour-transitive examples

- Fix $\mathcal{U} \subset \mathcal{V}$, $k \leq |\mathcal{U}|$, and write $\overline{\mathcal{U}} = \mathcal{V} \setminus \mathcal{U}$.
- Let $C = C(\mathcal{U}, k) := \binom{\mathcal{U}}{k}$, so $\mathrm{Aut}(C) = \mathrm{Sym}(\mathcal{U}) \times \mathrm{Sym}(\overline{\mathcal{U}})$
  - $C_1 = \{\gamma_1 \in \binom{\mathcal{V}}{k} \mid |\gamma_1 \cap \mathcal{U}| = k - 1\}$
  - C is neighbour-transitive
- Also if $|\mathcal{U}| < k$ then $C(\mathcal{U}, k) := \{$ all k-subsets containing $\mathcal{U}\}$ also neighbour-transitive

Comments on these [work with Bob Liebler]

Theorem These are all the neighbour-transitive examples with Aut(C) intransitive on V

1993, 2003 Meyerowitz classified all completely regular codes in J(v,k) of “strength zero” – they are precisely the intransitive neighbour-transitive examples!

Another set of known examples:

1994 Bill Martin "groupwise complete designs"

Partition $U = \{ U_1, U_2, \dots, U_b\}$ of V with $|U_i| = a$, and $b > 3$

Choose c with $1 < c$ at most $b/2$ and $k = bc$

Define C = all unions of c parts of U code in $J(v,k)$

1994 Bill determined which groupwise complete designs are completely regular codes in $J(v,k)$

Showed: if C in $J(v,k)$ completely regular and C is a 1-design but not a 2-design then C is a groupwise complete design

THE UNIVERSITY OF WESTERN AUSTRALIA
Achieve International Excellence

From now on this is work with Bob Liebler

Group of groupwise complete design C: Stab(U) = S_a wr S_b

Stab(U): always neighbour transitive on C

Bob and I: generalised g.c.d. construction – take any code C_0 in J(b,c) based on the b-set U and define

$$C = \{ \text{ union of all parts in } x \mid x \text{ in } C_0 \}$$

Theorem C is neighbour-transitive if C_0 is "strongly incidence transitive"

From now on this is work with Bob Liebler

Bob and I: take any code C_0 in J(b,c) based on the b-set U and define

$$C = \{ \text{ union of all parts in } x \mid x \text{ in } C_0 \}$$

5 more explicit constructions based on partition U of V
[a couple are completely transitive – discovered with Chris Godsil]

Theorem If C is neighbour-transitive in J(v,k) and Aut(C) is imprimitive on V (preserves some partition U) then C is one of these examples

From now on assume Aut(C) primitive on V

Theorem

Given $\mathrm{Aut}(C)$ is primitive on $\mathcal{V}$ and neighbour trans on C
(a) $\delta(C) \geq 3$ implies $\mathrm{Aut}(C)$ is 2-transitive on $\mathcal{V}$
(b) $\delta(C) \geq 2$ and C inc-trans implies $\mathrm{Aut}(C)$ is 2-trans on $\mathcal{V}$

Idea of Proof Strategy

- Let $\mathrm{u} \in \mathcal{V}$ and $\Delta(\mathrm{u}) = \cap\{\gamma \in C | \mathrm{u} \in \gamma\}$.
- Prove $\Delta(\mathrm{u})$ block of imprimitivity for $\mathrm{Aut}(C)$. Conclude $\Delta(\mathrm{u}) = \{\mathrm{u}\}$
- 'Use incidence-transitivity' to prove $\mathrm{Aut}(C)$ 2-trans.

Opens possibility to classify incidence-transitive codes with $\delta(C) \geq 2$, using classification of 2-transitive groups.

This is the 2-transitive reduction for neighbour transitive codes in J(v, k)

Still not complete – significant questions remain!

Already showed you sporadic case – complete classification

This leaves essentially four cases

- Projective
- Affine
- Rank 1 groups (Sz, Ree, unitary)
- Symplectic

Projective groups: G = Aut(C)

$$\mathrm{PSL}(n,q) \le G \le \mathrm{P\Gamma L}(n,q) \text{ with } \mathcal{V} = \mathrm{PG}(n-1,q)$$

Example $n = 2$ $\quad q = q_0^2$, $\gamma =$ Baer sub-line $\mathrm{PG}(1, q_0)$, $C = \gamma^G$

Theorem for $n = 2$

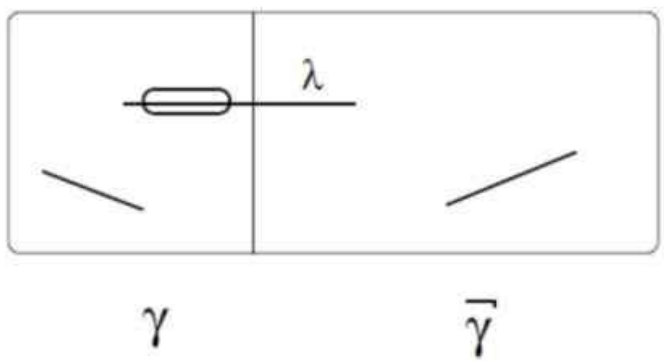
These are the only examples with $n = 2$, $k \ge 3$

Examples $n \ge 3$ $\quad \gamma =$ a subspace of $\mathrm{PG}(n-1,q)$, $C = \gamma^G$

Projective groups: G = Aut(C)

Theorem for $n \geq 3$: Either C as in the examples or

for each line λ of $\mathrm{PG}(n-1, q)$, $|\lambda \cap \gamma| \in \{0, x, q+1\}$ for x fixed, and moreover, either $x = 2$, or $q = q_0^2$ and $x = q_0 + 1$



Examples with $x = 2$

$C =$ the complements of r-subspaces in $\mathrm{PG}(n, 2)$ - any others?
Any with $q = q_0^2, x = q_0 + 1$? – Baer sub-geoms are not

Affine actions: G = Aut(C) in AΓL(n,q)

$$G \leq \mathrm{A\Gamma L}(n,q) \text{ with } \mathcal{V} = \mathrm{AG}(n,q)$$

Example $n = 1$ $\quad q = 4,\ \mathcal{V} = \mathbb{F}_4,\ C = \{\gamma = \{0,1\} = \mathbb{F}_2\},$

$C_1 = \{\{0,\xi\},\{0,\xi+1\},\{1,\xi\},\{1,\xi+1\}\}$

G generated by $t_1 : x \mapsto x+1$ and $\sigma : x \mapsto x^2$

Theorem for $n = 1$

This is the only example with $n = 1$ with G incidence-transitive

Proof is surprisingly difficult

The University of Western Australia
Achieve International Excellence

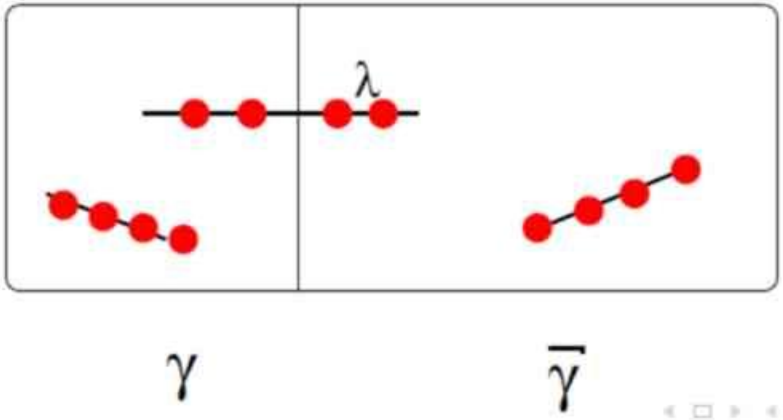
Affine actions: G = Aut(C) in AΓL(n,q)

Examples $n \geq 2$ $\quad \gamma =$ a subspace of $\mathrm{AG}(n, q)$, $C = \gamma^G$

Examples $n \geq 2$ $\quad q = 4$, $\gamma = \mathrm{AG}(n, 2)$ a Baer sub-geometry, $C = \gamma^G$

Theorem for $n \geq 2$: Either C as in the examples or

$q = 4$ and, for each line λ of $\mathrm{AG}(n, q)$, $|\lambda \cap \gamma| \in \{0, 2, 4\}$



Rank 1 groups: Ree, Sz, Unitary

- Sz(q) on V, $|V|=q^2+1$, $q=2^{2a+1}$ no examples

- Ree(q) on V, $|V|=q^3+1$, $q=3^{2a+1}$ no examples

- PSU(3, q) on V, $|V|=q^3+1$, examples from unital $k=q+1$

Symplectic groups G=Sp(2n,2) with |V|= $2^{n-1}(2^n+1)$ or $2^{n-1}(2^n-1)$

The University of Western Australia
Achieve International Excellence

$G = \mathrm{Sp}(n, 2)$ with $\mathcal{V} = \mathcal{Q}^\varepsilon$

set of non-degenerate quadratic forms of type $\varepsilon = \pm$ that polarise to the symplectic form preserved by G

Let $V(2n, 2)$ be the underlying space for natural G-action

Example $\mathcal{U}$ nonsingular so $V(2n, 2) = \mathcal{U} \perp \mathcal{U}^\perp$.

$\gamma = \{$ all forms $\varphi \in \mathcal{Q}^\varepsilon$ such that $\varphi|_\mathcal{U}, \varphi|_{\mathcal{U}^\perp}$ have types $\varepsilon_\mathcal{U}, \varepsilon_{\mathcal{U}^\perp}$ where $\varepsilon_\mathcal{U}\varepsilon_{\mathcal{U}^\perp} = \varepsilon \}$

So that's it:

- Several open problems
- Affine and projective cases: Very symmetrical geometrical configurations - do they exist?
- Symplectic groups: huge analytical issues – orthogonal model
- Ways forward?
  - Computation for small n
  - Use geometry and algebra for better understanding
  - Use knowledge of maximal subgroups to restrict possibilities