

Permutation decoding for codes from designs, finite geometries and 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@clermson.edu
www.math.clemson.edu/~keyj

ASI Croatia June 2010

Abstract

Permutation decoding was introduced by **MacWilliams** [Mac64] in the early 60's. It can be used when a linear code has a sufficiently large automorphism group to ensure the existence of a set of automorphisms, called a PD-set, that has some specified properties.

This series of talks will describe the method and some recent developments in finding PD-sets for codes defined through the row-span over finite fields of incidence matrices of classes of designs or graphs, and adjacency matrices of classes of regular graphs.

These codes have many properties that can be deduced from the combinatorial properties of the designs or graphs, and often have a great deal of symmetry and large automorphism groups.

- 1 Permutation decoding
 - Coding terminology
 - Algorithm for permutation decoding
 - Lower bound on the size of a PD-set
- 2 Background and terminology
 - Designs
 - Codes from designs
 - Finite geometries
 - Graphs
 - Finding PD-sets
- 3 Codes from graphs: Examples
- 4 Codes from finite geometries: Example
- 5 Some other results
- 6 References

Permutation decoding

Linear codes terminology

- A **linear code** is a subspace of a finite-dimensional vector space over a finite field. (All codes are linear here.)
- The **weight**, $\text{wt}(x)$, of a vector x is the number of non-zero coordinate entries. If a code has smallest non-zero weight d then the code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ 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 a $[n, k, d]_q$ code C 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. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$.
- A code C is **self-orthogonal** if $C \subseteq C^\perp$ and is **self-dual** if $C = C^\perp$.

Linear codes terminology continued

- A **check** matrix for C is a generator matrix H for C^\perp .
- The **syndrome** of a vector $y \in F^n$ is Hy^T .
- 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 $[I_k | A]$; a check matrix then is given by $[-A^T | I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n - k$ coordinates are the **check symbols**.

Permutation decoding

From [Huf98, Mac64, MS83] and [KMM05, KV05]

Definition

C is a t -error-correcting code with information set \mathcal{I} and check set \mathcal{C} . 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 $s \leq t$ 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} .

In particular, if $\mathcal{I} = \{1, \dots, k\}$ and $\mathcal{C} = \{k + 1, \dots, n\}$, then every s -tuple from $\{1, \dots, n\}$ can be moved by some element of \mathcal{S} into \mathcal{C} .

Algorithm for permutation decoding

C is a $[n, k, d]_q$ code where $d = 2t + 1$ or $2t + 2$.

$G = [I_k | A]$ is a $k \times n$ generator matrix for C :

Any k -tuple v is encoded as vG .

The first k columns are the information symbols, the last $n - k$ are check symbols.

$H = [-A^T | I_{n-k}]$ is an $(n - k) \times n$ check matrix for C :

$\mathcal{S} = \{g_1, \dots, g_m\}$ is a PD-set for C , written in some chosen order.

Suppose x is sent and y is received and at most t errors occur:

- for $i = 1, \dots, m$, compute yg_i and the syndrome $s_i = H(yg_i)^T$ until an i is found such that the weight of s_i is t or less;
- if $u = u_1 u_2 \dots u_k$ are the information symbols of yg_i , compute the codeword $c = uG$;
- decode y as cg_i^{-1} .

Why permutation decoding works

Result

Let C be an $[n, k, d]_q$ t -error-correcting code.

Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the check positions.

Let $y = c + e$ be a vector in \mathbb{F}_q^n , where $c \in C$ and e has weight $\leq t$.

Then the information symbols in y are correct if and only if

$$wt(Hy^T) \leq t.$$

Proof: Suppose C has generator matrix G in standard form, i.e. $G = [I_k | A]$ and that the encoding is done using G , i.e. the data set $x = (x_1, \dots, x_k)$ is encoded as xG .

The information symbols of a vector in \mathbb{F}_q^n are the first k symbols.

The check matrix is $H = [-A^T | I_{n-k}]$.

Suppose the information symbols of $y = c + e$ are correct, $c \in C$. Then

$$Hy^T = H(c^T + e^T) = He^T = e^T,$$

since the first k coordinates of e are 0. Thus $\text{wt}(Hy^T) \leq t$.

Proof continued

Conversely, suppose that not all the information symbols are correct. Then if $e = e_1 \dots e_n$, and $e' = e_1 \dots e_k$, $e'' = e_{k+1} \dots e_n$, we assume that e' is not the zero vector. Now use the fact that for any vectors

$$\text{wt}(x + y) \geq \text{wt}(x) - \text{wt}(y).$$

Then

$$\begin{aligned} \text{wt}(Hy^T) &= \text{wt}(He^T) = \text{wt}(-A^T e'^T + e''^T) \\ &\geq \text{wt}(-A^T e'^T) - \text{wt}(e''^T) = \text{wt}(e'A) - \text{wt}(e'') \\ &= \text{wt}(e'A) + \text{wt}(e') - \text{wt}(e') - \text{wt}(e'') = \text{wt}(e'G) - \text{wt}(e) \\ &\geq d - t \geq t + 1 \end{aligned}$$

since $d \geq 2t + 1$, which proves the result. ■

Minimum size for a PD-set

Counting shows that there is a minimum size a PD-set can have; most the sets known have size larger than this minimum. The following is due to Gordon [Gor82], using a result of Schönheim [Sch64]:

Result

If S is a PD-set for a t -error-correcting $[n, k, d]_q$ code C , and $r = n - k$, then

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \dots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \dots \right\rceil \right\rceil \right\rceil.$$

(Proof in Huffman [Huf98].)

This result can be adapted to s -PD-sets for $s \leq t$ by replacing t by s in the formula.

Example meeting bound

Example: The binary extended Golay code, parameters $[24, 12, 8]$, has $n = 24$, $r = 12$ and $t = 3$, so

$$|\mathcal{S}| \geq \left\lceil \frac{24}{12} \left\lceil \frac{23}{11} \left\lceil \frac{22}{10} \right\rceil \right\rceil \right\rceil = 14$$

and PD-sets of this size has been found (see Gordon [Gor82] and Wolfmann [Wol83]).

Designs, geometries and graphs

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, or $(\mathcal{P}, \mathcal{B})$, with point set \mathcal{P} , block set \mathcal{B} and incidence $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$, is a t - (v, k, λ) **design**, if

- $|\mathcal{P}| = v$,
- every block $B \in \mathcal{B}$ is incident with precisely k points,
- every t distinct points are together incident with precisely λ blocks.

Codes from designs

- The **code of the design \mathcal{D} over the finite field F** is the space spanned by the incidence vectors of the blocks over F .
- If $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ and $Q \subseteq \mathcal{P}$, then

$$v^Q$$

is the **incidence vector** of Q .

- Thus the **code of a design over F** is

$$C = \langle v^B \mid B \in \mathcal{B} \rangle,$$

and is a subspace the full vector space $F^{\mathcal{P}}$ of functions from \mathcal{P} to F .

Finite geometries

\mathbb{F}_q denotes the finite field of order q .

- The set of points and r -dimensional subspaces of an m -dimensional projective geometry forms a 2-design $PG_{m,r}(\mathbb{F}_q)$.
- The set of points and r -dimensional flats of an m -dimensional affine geometry forms a 2-design, $AG_{m,r}(\mathbb{F}_q)$.
- The **automorphism groups** of these designs (and codes) are the full projective or affine semi-linear groups, $P\Gamma L_{m+1}(\mathbb{F}_q)$ or $A\Gamma L_m(\mathbb{F}_q)$, and are 2-transitive on points.
- If $q = p^e$ where p is a prime, the codes of these designs are over \mathbb{F}_p and are subfield subcodes of the **generalized Reed-Muller codes** and the dimension and minimum weight is known in each case: see [AK92, Theorem 5.7.9].

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, so $x \sim y$, $[\mathbf{x}, \mathbf{y}]$ denotes the edge in E between them.
- 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.

- The **neighbourhood design** of a regular graph of valency k is the $1-(N, k, k)$ symmetric design formed by taking the points to be the vertices, and the blocks to be the sets of neighbours of a vertex, for each vertex.
- An **incidence matrix** of Γ 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 Γ is regular with valency k , then the $1-(\frac{Nk}{2}, k, 2)$ design with incidence matrix B is called the **incidence design** of Γ .
- 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 Γ share a vertex in V .

- The **code** of Γ over F_p is the row span of an adjacency matrix A over F_p , denoted $C_p(\Gamma) = C_p(A) = C_p(\mathcal{D})$, where \mathcal{D} is the neighbourhood design. So $\dim(C_p(\Gamma)) = \text{rank}_p(A)$.
- If B is an incidence matrix for Γ , $C_p(B)$ is $C_p(\mathcal{G})$ where \mathcal{G} is the incidence design if Γ is regular.
- If $[x_i, x_{i+1}]$ for $i = 1$ to $r - 1$, and $[x_r, x_1]$ are all edges of Γ , and the x_i are all distinct, then the sequence written (x_1, \dots, x_r) will be called a **closed path** of length r for Γ .

Line graphs

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

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

So, for the binary code, $C_2(L(\Gamma)) \subseteq C_2(B)$. These equations tell us little for codes over \mathbb{F}_p for p odd.

However, we get nothing more of interest from $C_p(L(\Gamma))$ when p is odd, because ...

Codes from adjacency matrices of line graphs

$\Gamma = (V, E)$, $\mathcal{D}(\Gamma)$ its neighbourhood design.

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

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

Lemma

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:

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



Finding PD-sets

- First we need an **information set**. These are not known in general. Different information sets will yield different possibilities for PD-sets, and for some information sets there can be no PD-set.
- For symmetric designs with a symmetric incidence matrix (e.g. desarguesian projective planes), a basis of incidence vectors of blocks will yield a corresponding information set, by duality. This links to the question of finding **bases of minimum-weight vectors** in the geometric case, again something not known in general.
- For **planes**, Moorhouse [Moo91] or Blokhuis and Moorhouse [BM95] give bases in the prime-order case. For the designs of **points and hyperplanes of prime order** see [KMM06]

NOTE: **Magma** [CSW06, BCP97] has been a great help in looking at small cases to get the general idea of what to might hold for the general case and infinite classes of codes.

Cyclic codes and generalizations

MacWilliams [Mac64] found PD-sets for cyclic codes.

An $[n, k, d]_q$ code C is cyclic if whenever $c = c_1c_2 \dots c_n \in C$ then every cyclic shift of c is in C . So $\tau \in S_n$ defined by

$$\tau : i \mapsto i + 1$$

for $i \in \{1, 2, \dots, n\}$, is in the automorphism group of C , and $\tau^n = 1$.

If a message c is sent and t errors occur, then if e is the error vector and if there is a sequence of k zeros between two of the error positions, then τ^j for some j will move the sequence of zeros into the information positions, and thus the t errors will be in the check positions.

Thus the **cyclic** group $\langle \tau \rangle$ will be a PD-set for C if $k < \frac{n}{t}$.

Result ([KMM06])

Let $C = [n, k, d]_p$, \mathcal{I} an information set, \mathcal{C} the corresponding check set and $G \leq \text{Aut}(C)$.

Let $m = \max(|\mathcal{O} \cap \mathcal{I}|/|\mathcal{O}|)$ over the G -orbits \mathcal{O} .

If $s = \min(\lceil \frac{1}{m} \rceil - 1, \lfloor \frac{d-1}{2} \rfloor)$, then G is an s -PD-set for C .

This result is true for any information set.

If the group G is **transitive** then $m = k/n$.

Thus sharply 1-transitive subgroups would be best for this result.

Incidence matrix for a graph

Result 3 is applicable to codes from incidence matrices of connected regular graphs with automorphism groups transitive on edges:

Result ([FKM])

Let $\Gamma = (V, E)$ be a regular graph of valency k with an automorphism group A transitive on edges.

Let G be an incidence matrix for Γ . If, for p a prime,

$$C_p(\Gamma) = [|E|, |V| - \epsilon, k]_p,$$

where $\epsilon \in \{0, 1, \dots, |V| - 1\}$, then any transitive subgroup of A will serve as a PD-set for full error correction for $C_p(\Gamma)$.

This is used in the following sections discussing PD-sets for some classes of graphs.

NOTE:

Individual codes from designs, graphs or elsewhere can be studied or computed with the help of Magma [CSW06, BCP97], and information sets, and PD-sets, or s -PD-sets found.

Our interest here is with general methods that apply to infinite classes of designs or graphs, or finite geometries.

Classes of graphs

Codes from adjacency and incidence matrices for the classes:

- Triangular graphs $L(K_n)$ and incidence designs of K_n ;
- Lattice graphs $L(K_{n,n})$ and incidence designs of $K_{n,n}$;
- Rectangular lattice graphs $L(K_{n,m})$;
- Line graphs of complete multi-partite graphs K_n^m ;
- Paley graphs;
- Uniform subset graphs on 3-sets;
- Hamming graphs $H^k(n, m)$.

Classes of finite geometries

- Desarguesian affine and projective planes of prime order;
- $C_p(AG_{3,1}(\mathbb{F}_p))$ for p prime;
- $C_p(AG_{m,m-1}(\mathbb{F}_p))$ and $C_p(PG_{m,m-1}(\mathbb{F}_p))$ for p prime;
- First- and second-order Reed Muller codes.

Example from a class of graphs

EXAMPLE: Lattice graph, $L_2(n) = L(K_{n,n})$

From [KR, KS08]

The lattice graph $L_2(n)$ is the line graph of the complete bipartite graph $K_{n,n}$. We will try permutation decoding on $C_2(L_2(n))$, but first look at the p -ary code of the incidence design of $K_{n,n}$.

For $n \geq 2$, let \mathcal{G}_n be the $1-(n^2, n, 2)$ incidence design of $K_{n,n}$.

The point set of \mathcal{G}_n is $\mathcal{P}_n = A \times B$, where

$A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$,

i.e. the edges of $K_{n,n}$.

An incidence matrix G_n has first n rows labelled by the vertices of $K_{n,n}$ in A , and the next n rows by B . The columns are labelled

$$[a_1, b_1], \dots, [a_1, b_n], [a_2, b_1], \dots, [a_2, b_n], \dots, [a_n, b_1], \dots, [a_n, b_n]. \quad (1)$$

For $a_i \in A$, $b_i \in B$ the blocks of \mathcal{G}_n defined by the rows a_i and b_i are denoted

$$\bar{a}_i = \{[a_i, b_j] \mid 1 \leq j \leq n\}, \quad \bar{b}_i = \{[a_j, b_i] \mid 1 \leq j \leq n\}.$$

$C_p(\mathcal{G}_n)$ is the row span of G_n over \mathbb{F}_p .

$L_2(n)$

The lattice graph $L_2(n)$ is the line graph $L(K_{n,n})$. The rows of an adjacency matrix M_n for $L_2(n)$ give the blocks of the neighbourhood design $\overline{\mathcal{D}}_n$ of $L_2(n)$. We have

- $G_n^T G_n = M_n + 2I_{n^2}$.
- The blocks of $\overline{\mathcal{D}}_n$ (rows of M_n) are

$$\overline{[a_i, b_j]} = \{[a_i, b_k] \mid k \neq j\} \cup \{[a_k, b_j] \mid k \neq i\}$$

for each point $[a_i, b_j] \in \mathcal{P}_n$.

- $\overline{\mathcal{D}}_n$ is a symmetric 1 - $(n^2, 2(n-1), 2(n-1))$ design for $n \geq 2$.
- $K_{n,n}$ has closed paths of length 4, so, by Lemma 2, only $C_p(L_2(n))$ for $p = 2$ is of any use, and then $C_2(L_2(n)) \subseteq C_2(\mathcal{G}_n)$.

Automorphism groups

The group $G = S_n \wr S_2$ is the automorphism group of $K_{n,n}$.

It acts on the edge set $\mathcal{P}_n = A \times B$ by its construction as an extension of the group $H = S_n \times S_n$ by $S_2 = \{1, \tau\}$, where $\tau = (1, 2)$. The element τ then acts on H via $(\alpha, \beta)^\tau = (\beta, \alpha)$, for $\alpha, \beta \in S_n$.

Then G acts as a rank-3 group on \mathcal{P}_n as follows:

$$[a_i, b_j]^{(\alpha, \beta)} = [a_{i\alpha}, b_{j\beta}], \text{ and } [a_i, b_j]^\tau = [a_j, b_i]. \quad (2)$$

Furthermore, G acts on each of these graphs, designs and codes.

Let $\Omega = \{1, \dots, n\}$.

Lemma

For $n \geq 2$, if $\{i, j, k, m\} \subseteq \Omega$ where $i \neq k$, and $j \neq m$, then the vector

$$u = u([a_i, b_j], [a_k, b_m]) = v^{[a_i, b_j]} + v^{[a_k, b_m]} - v^{[a_i, b_m]} - v^{[a_k, b_j]} \quad (3)$$

is in $C_p(\mathcal{G}_n)^\perp$ for any prime p .

Proof: This is clear since $(\bar{x}, u) = 0$ for all choices of $x \in A \cup B$, recalling that

$$\bar{a}_i = \{[a_i, b_j] \mid 1 \leq j \leq n\}, \quad \bar{b}_i = \{[a_j, b_i] \mid 1 \leq j \leq n\}.$$



Codes from \mathcal{G}_n continued

Proposition

For $n \geq 2$, any prime p ,

$$C_p(\mathcal{G}_n) = [n^2, 2n - 1, n]_p,$$

where \mathcal{G}_n is the incidence design of $K_{n,n}$.

For $n \geq 3$ the minimum-weight vectors are the scalar multiples of the incidence vectors of the blocks of \mathcal{G}_n .

Proof: It is easy to see that the incidence matrix G_n has rank $2n - 1$ over any field; clearly the minimum weight is at most n .

Now let \mathcal{B}_n be the set of supports of the vectors $u([a_i, b_j], [a_k, b_m])$ as defined in Equation (3). Then $(\mathcal{P}_n, \mathcal{B}_n)$ is a $1-(n^2, 4, r)$ design, where $r = (n - 1)^2$.

Proof continued

Let $w \in C_n$ and $\text{Supp}(w) = S$, where $|S| = s$. Let $P \in S$. We first count the number of blocks of \mathcal{B}_n through P and another point Q .

Recall that

$$u = u([a_i, b_j], [a_k, b_m]) = v^{[a_i, b_j]} + v^{[a_k, b_m]} - v^{[a_i, b_m]} - v^{[a_k, b_j]}.$$

Suppose $P = [a_i, b_j]$. Then

- 1 if $Q = [a_i, b_k]$ then $P, Q \in \text{Supp}(u([a_i, b_j], [a_m, b_k]))$ for all $m \neq i$, giving $n - 1$ such blocks;
- 2 if $Q = [a_m, b_j]$ then P, Q are on $n - 1$ blocks again;
- 3 if $Q = [a_m, b_k]$ where $m \neq i, k \neq j$, then $P, Q \in \text{Supp}(u([a_i, b_j], [a_m, b_k]))$, giving just one block.

Proof continued

Suppose that in \mathcal{S} there are k points of the type $[a_i, b_k]$ or $[a_m, b_j]$, and ℓ of the type $[a_m, b_k]$ where $m \neq i, k \neq j$. 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 $i \geq 5$.

Thus $r = z_2 + z_3 + z_4$ and, counting incidences,

$$z_2 + 2z_3 + 3z_4 = (n-1)k + \ell = (n-1)(s-\ell-1) + \ell = (n-1)(s-1) - \ell(n-2).$$

So $r = (n-1)^2 \leq (n-1)(s-1) - \ell(n-2) \leq (n-1)(s-1)$ for $n \geq 2$.

It follows that $s \geq n$ for $n \geq 2$, and the minimum weight is n .

Proof continued

Need to show that for $n \geq 3$ the vectors of weight n are the scalar multiples of the blocks of \mathcal{G}_n . Recall that $P = [a_i, b_j]$.

Suppose $s = n$ with the same notation as above. Putting $s = n$ in the equations we get

$$(n-1)^2 \leq z_2 + 2z_3 + 3z_4 = (n-1)^2 - (n-2)\ell.$$

Since $n-2 > 0$ this implies that $\ell = 0$, and

$r = z_2 + z_3 + z_4 = z_2 + 2z_3 + 3z_4$. Thus $z_3 = z_4 = 0$, $k = n-1$ and $\mathcal{S} \setminus \{P\}$ consists of at least $n-1 \geq 2$ points and they are all of the form $[a_i, b_k]$ or $[a_m, b_j]$.

Suppose there are k_1 of the form $[a_i, b_k]$ and k_2 of the form $[a_m, b_j]$. If $k_1 = 0$ or $k_2 = 0$ then $\mathcal{S} = \overline{a_i}$ or $\overline{b_j}$. If $k_1, k_2 \geq 1$ then we can make the same counting argument using the point $[a_i, b_k]$ for P and get a contradiction for $\ell = 0$.

Thus $\mathcal{S} = \overline{a_i}$, say. If $w \neq \alpha v^{\overline{a_i}}$ for some $\alpha \in \mathbb{F}_p$ then $\text{wt}(w + \beta v^{\overline{a_i}}) < n$ for some $\beta \in \mathbb{F}_p$, contradicting the minimum weight being n . ■

Proposition

If $C_n = C_p(\mathcal{G}_n)$ where $n \geq 3$, and p is any prime, then

$$\mathcal{I}_n = \{[a_i, b_n] \mid 1 \leq i \leq n\} \cup \{[a_n, b_i] \mid 1 \leq i \leq n-1\}$$

is an information set for C_n and the set

$$S = \{((n, i), (n, i)) \mid 1 \leq i \leq n\},$$

of elements of $S_n \times S_n$, where $(i, j) \in S_n$ is a transposition and (k, k) is the identity of S_n , is a PD-set for C_n of size n for the information set \mathcal{I}_n .

Proof: That \mathcal{I}_n is an information set follows easily. Let \mathcal{C}_n be the corresponding check set.

To prove that S is a PD-set for \mathcal{C}_n , note that \mathcal{C}_n can correct $t = \lfloor \frac{n-1}{2} \rfloor$ errors. Let

$$\mathcal{T} = \{[a_{i_1}, b_{j_1}], \dots, [a_{i_t}, b_{j_t}]\}$$

be a set of t points of \mathcal{P}_n , and

$$\Omega_1 = \{i_1, \dots, i_t\}, \Omega_2 = \{j_1, \dots, j_t\}, \mathcal{O} = \Omega_1 \cup \Omega_2.$$

Then since $t \leq \frac{n-1}{2}$, $|\mathcal{O}| \leq 2t \leq n-1$.

If $n \notin \mathcal{O}$ then we use the identity ι .

If $n \in \mathcal{O}$ then there is a $k \in \Omega$, $k \neq n$, such that $k \notin \mathcal{O}$ and the element $((n, k), (n, k))$ will move \mathcal{T} into \mathcal{C}_n .

Thus S is a PD-set. ■

NOTE: Result 2 gives the bounds $\frac{n}{2}$ for n even, and $\frac{n+3}{2}$ for n odd for the smallest size possible for a PD-set.

$C_2(L_2(n))$

From $G_n^T G_n = M_n + 2I_{n^2}$, where M_n is an adjacency matrix for $L_2(n)$ we get $C = C_2(M_n) \subseteq C_2(G_n)$.

Let V be the row span of G_n^T over \mathbb{F}_2 . Then $\dim(V) = 2n - 1$. The map $\tau : V \rightarrow C$ is defined by $\tau : v = (v_1, \dots, v_{2n}) \mapsto (v_1, \dots, v_{2n})G_n$, so that $V\tau = C$ and $\dim(C) + \dim \ker(\tau) = \dim(V) = 2n - 1$. A vector v is in the kernel if and only if $v \in V$ and $vG_n = \mathbf{0}$, and since $jG_n = \mathbf{0}$, where $j = j_{2n}$, we need to see if $j \in V$. This is easy to prove, so $\dim(C) = 2n - 2$.

Let $E_n = \{ v^{\bar{x}} - v^{\bar{y}} \mid x, y \in A \cup B \}$.

Then $C_2(L_2(n)) = C_2(E_n)$, the row span of E_n over \mathbb{F}_2 .

More generally, consider $C_p(E_n)$, any prime p .

Proposition

For $n \geq 3$, any prime p , $C_p(E_n) = [n^2, 2n - 2, 2n - 2]_p$ and the words of weight $2n - 2$ are the scalar multiples of $v^{\overline{a_i}} - v^{\overline{b_j}}$, for $1 \leq i, j \leq n$.

Proof: To be found in [KR].

In particular, this is true for $C_2(L_2(n)) = C_2(E_n)$.
(See also [Ton88, HPvR99])

PD-sets for $C_p(E_n)$

Proposition

For $n \geq 3$, p any prime,

$$\mathcal{I}_n^* = \{[a_i, b_n] \mid 2 \leq i \leq n\} \cup \{[a_n, b_i] \mid 1 \leq i \leq n-1\}$$

is an information set for $C_p(E_n)$ and the set

$$S = \{((n, i), (n, j)) \mid 1 \leq i, j \leq n\}, \quad (4)$$

of elements of $S_n \times S_n$, where $(i, j) \in S_n$ is a transposition and (k, k) is the identity of S_n , is a PD-set of size n^2 for $C_p(E_n)$ using \mathcal{I}_n^* .

Proof: That \mathcal{I}_n^* is an information set follows easily. Let \mathcal{C}_n be the corresponding check set. To prove that S is a PD-set for $C_p(E_n)$, note that the code can correct up to $n - 2$ errors. Let

$$\mathcal{T} = \{[a_{i_1}, b_{j_1}], \dots, [a_{i_t}, b_{j_t}]\}$$

be a set of $t \leq n - 2$ points of \mathcal{P}_n , and

$$\Omega_1 = \{i_1, \dots, i_t\}, \Omega_2 = \{j_1, \dots, j_t\}, \mathcal{O} = \Omega_1 \cup \Omega_2.$$

If $n \notin \mathcal{O}$ then we use the identity ι .

Otherwise, since $t \leq n - 2$ there is a $k \neq n$, $k \notin \Omega_1$ and an $\ell \neq n$, $\ell \notin \Omega_2$, and $((n, k), (n, \ell))$ will move \mathcal{T} into \mathcal{C}_n . Thus S is a PD-set, of size n^2 . ■

NOTE: This is the PD-set used in the binary case in [KS08].

Result 2 gives a bound linear in n .

Time complexity of permutation decoding

The **worst-case time complexity** for the decoding algorithm using an s -PD-set of size m on an $[n, k, d]_q$ code is $\mathcal{O}(nkm)$.

So we want **small** PD-sets.

Since the algorithm uses an **ordering** of the PD-set, good choices of the ordering of the elements can reduce the complexity.

For example:

find an s -PD-set S_s for each $0 \leq s \leq t$ such that

$$S_0 < S_1 \dots < S_t$$

and arrange the PD-set S in this order:

$$S_0 \cup (S_1 \setminus S_0) \cup (S_2 \setminus S_1) \cup \dots \cup (S_t \setminus S_{t-1}).$$

(Usually take $S_0 = \{id\}$).

Complexity of permutation decoding

The following can be used to order the PD-set for the binary code of the square lattice graph.

Result ([Sen07])

For the $[n^2, 2(n-1), 2(n-1)]_2$ code from the lattice graph $L_2(n)$, using the information set

$$\mathcal{I}_n^* = \{[a_i, b_n] \mid 2 \leq i \leq n-1\} \cup \{[a_n, b_i] \mid 1 \leq i \leq n\},$$

for $0 \leq k \leq t = n-2$,

$$S_k = \{((i, n), (j, n)) \mid n-k \leq i, j \leq n\}$$

is a k -PD-set.

((n, n) is the identity permutation in S_n .)

Complexity of permutation decoding

Thus ordering the elements of the PD-set as

$$S_0, S_1 \setminus S_0, S_2 \setminus S_1, \dots, S_{n-2} \setminus S_{n-3}$$

will result in a PD-set where, if $s \leq t = n - 2$ errors occur then the search through the PD-set need only go as far as s^{th} block of elements. Since the probability of less errors is highest, this will reduce the time complexity.

Example from another class of graphs

Incidence matrices of Paley graphs

Let q be a prime power with $q \equiv 1 \pmod{4}$.

The **Paley graph**, denoted by $P(q)$, has the finite field \mathbb{F}_q of order q as vertex set and two vertices x and y are adjacent if and only if $x - y$ is a non-zero square in \mathbb{F}_q .

The Paley graph is a strongly regular graph of type $(q, \frac{q-1}{2}, \frac{q-1}{4} - 1, \frac{q-1}{4})$ and is isomorphic to its complement.

Codes from the incidence matrices of Paley graphs

In [GK] it is shown that

Result

Let $\Gamma = P(q)$ where $q \geq 9$, q a prime power, and $q \equiv 1 \pmod{4}$.

Let \mathcal{G}_q be the $1 - (\frac{q(q-1)}{4}, \frac{q-1}{2}, 2)$ incidence design of $P(q)$.

Then $C = C_2(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q-1, \frac{q-1}{2}]_2$ and for p odd,

$C = C_p(\mathcal{G}_q) = [\frac{q(q-1)}{4}, q, d]_p$ where $\frac{q-1}{2} \geq d \geq \frac{q-1}{2} - 1$.

For all p , C can correct $\frac{q-5}{4}$ errors.

This is proved using a combinatorial argument involving the weight-4 vectors from closed paths of length 4.

Automorphism group

Let $q = q_1^e$ for some prime q_1 . For any $\sigma \in \text{Aut}(\mathbb{F}_q)$ and $a, b \in \mathbb{F}_q$ with a a non-zero square, we define the map $\tau_{a,b,\sigma}$ on \mathbb{F}_q by

$$\tau_{a,b,\sigma} : x \mapsto ax^\sigma + b, \quad (5)$$

for $x \in \mathbb{F}_q$. Then

$$A_q = \{\tau_{a,b,\sigma} \mid \sigma \in \text{Aut}(\mathbb{F}_q), a, b \in \mathbb{F}_q, a \text{ a non-zero square}\} \quad (6)$$

is the automorphism group of $P(q)$, of order $\frac{1}{2}eq(q-1)$.

The group A_q acts on \mathcal{G}_q and is transitive on points (edges of $P(q)$).

Information sets for q prime

Result

The Paley graph $P(q)$ for $q \geq 9$, $q \equiv 1 \pmod{4}$ is Hamiltonian and if (x_1, \dots, x_q) is a closed path of length q , $x_i \neq x_j$ for $i \neq j$, then

$$\mathcal{I} = \{[x_1, x_2], [x_2, x_3], \dots, [x_{n-1}, x_n], [x_n, x_1]\}$$

is an information set for $C_p(\mathcal{G}_q)$ for p odd, and $\mathcal{I} \setminus \{[x_n, x_1]\}$ is an information set for $C_2(\mathcal{G}_q)$.

In particular, if q is a prime, then

$$(0, 1, \dots, q-1)$$

is a Hamiltonian path.

PD-sets for q prime

When q is a prime, $\sigma = 1$, the identity map, so write

$$\tau_{a,b} = \tau_{a,b,1}$$

in the notation of Equation (5).

If $\mathbb{F}_q^* = \langle w \rangle$ and $K_q = \langle w^2 \rangle$, the subgroup of squares in the multiplicative group of the field, of order $\frac{q-1}{2}$, we write

$$T_q = \{\tau_{1,b} \mid b \in \mathbb{F}_q\} \quad \text{and} \quad Q_q = \{\tau_{a,0} \mid a \in K_q\}. \quad (7)$$

Then $A_q = T_q \rtimes Q_q$, and T_q is the group of translations.

Proposition ([GK])

Let q be a prime with $q \equiv 1 \pmod{4}$, $P(q)$ the Paley graph on \mathbb{F}_q , \mathcal{G}_q its incidence design. Let

$$\mathcal{I} = \{[0, 1], [1, 2], \dots, [q - 1, 0]\}, \quad \mathcal{I}^* = \mathcal{I} \setminus \{[q - 1, 0]\}.$$

Then Q_q of Equation (7) is a PD-set of size $\frac{q-1}{2}$ for $C_p(\mathcal{G}_q)$ for any prime p with information set \mathcal{I} for p odd, or information set \mathcal{I}^* for $p = 2$.

Proof

Proof: For all p , $C = C_p(\mathcal{G}_q)$ corrects $t = \frac{q-5}{4}$ errors, by Result 6.

Let \mathcal{C} denote the check positions corresponding to \mathcal{I} . We wish to find an element of Q_q that will take a given t -set of points into \mathcal{C} .

Let $u = w^2$. The points of \mathcal{G}_q are of the form $[x, x + u^k]$ where $0 \leq k \leq \frac{q-1}{2} - 1$, and a point is in \mathcal{I} if and only if $k = 0$. Let

$$\mathcal{T} = \{[x_i, x_i + u^{k_i}] \mid 1 \leq i \leq t\}$$

be a set of t points. If $\mathcal{T} \subseteq \mathcal{C}$ then we can use the identity map $\tau_{1,0}$. Otherwise, since

$$[x_i, x_i + u^{k_i}]_{\tau_{u^\ell, 0}} = [x_i u^\ell, x_i u^\ell + u^{k_i + \ell}],$$

where $0 \leq \ell \leq \frac{q-1}{2} - 1$, if we can choose ℓ such that $k_i + \ell \neq 0$ for all $1 \leq i \leq t$, then all the points will move into \mathcal{C} . Since $t = \frac{q-5}{4}$ and ℓ can be chosen from $\frac{q-1}{2} - 1$ values (since $\ell \neq 0$), we can clearly find such an ℓ for any t -set of points. This argument works for all primes p , taking \mathcal{I}^* in the binary case. ■

Example from finite geometries

Codes from finite geometries

If $q = p^e$ where p is prime, the code of the **desarguesian projective plane** $PG_2(\mathbb{F}_q)$ of order q has parameters: $[q^2 + q + 1, (\frac{p(p+1)}{2})^e + 1, q + 1]_p$.

For the **desarguesian affine plane** $AG_2(\mathbb{F}_q)$, the code is $[q^2, (\frac{p(p+1)}{2})^e, q]_p$. Similarly, the designs formed from points and subspaces of dimension r in projective or affine space, have codes whose parameters are known.

The codes are subfield subcodes of the **generalized Reed-Muller codes**, and the automorphism groups are the semi-linear groups and doubly transitive on points.

Finite desarguesian planes

Thus 2-PD-sets (in fact also 3- and 4-PD-sets) always exist but the bound for full error-correction of Result 2 is greater than the size of the group (see [KMM05]) as q gets large, so beyond these bounds PD-sets for full error correction **cannot exist**:

E.g., for projective desarguesian planes correcting $\lfloor \frac{q+1}{2} \rfloor$ errors:

$q = p$ prime and $p > 103$;

$q = 2^e$ and $e > 12$;

$q = 3^e$ and $e > 6$;

$q = 5^e$ and $e > 4$;

$q = 7^e$ and $e > 3$;

$q = 11^e$ and $e > 2$;

$q = 13^e$ and $e > 2$;

$q = p^e$ for $p > 13$ and $e > 1$.

Similar results hold for the affine and dual cases, in all of the designs.

EXAMPLE: $C_p(AG_2(\mathbb{F}_p))$

Find 3-PD-sets for $C_p(AG_2(\mathbb{F}_p)) = [p^2, \binom{p+1}{2}, p]_p$, p prime, using the fact that it is the generalized Reed-Muller code, $\mathcal{R}_{\mathbb{F}_p}(p-1, 2)$. Take $p \geq 7$ so that the code will correct at least 3 errors.

Need an information set.

Generalized Reed-Muller codes

The ρ^{th} -order generalized Reed-Muller code $\mathcal{R}_{\mathbb{F}_q}(\rho, m)$, of length q^m over the field \mathbb{F}_q is defined to be

$$\langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid 0 \leq i_k \leq q - 1, \text{ for } 1 \leq k \leq m, \sum_{k=1}^m i_k \leq \rho \rangle.$$

In particular, $\mathcal{R}_{\mathbb{F}_p}((m - r)(p - 1), m)$ is the p -ary code of the affine geometry design $AG_{m,r}(\mathbb{F}_p)$ of points and r -flats of $AG_m(\mathbb{F}_p)$, p prime. In [KMM06] we found information sets for these codes:

Result ([KMM06])

Let $V = \mathbb{F}_q^m$, where $q = p^t$ and p is a prime, and $\mathbb{F}_q = \{\alpha_0, \dots, \alpha_{q-1}\}$. Then

$$\mathcal{I} = \{(\alpha_{i_1}, \dots, \alpha_{i_m}) \mid \sum_{k=1}^m i_k \leq \nu, 0 \leq i_k \leq q-1\}$$

is an information set for $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$.

If $q = p$ is a prime,

$$\mathcal{I} = \{(i_1, \dots, i_m) \mid i_k \in \mathbb{F}_p, 1 \leq k \leq m, \sum_{k=1}^m i_k \leq \nu\}$$

is an information set for $\mathcal{R}_{\mathbb{F}_p}(\nu, m)$, by taking $\alpha_{i_k} = i_k$.

Example to illustrate the result

$q = 3$		0	0	0	1	1	2	1	2	2
$m = 2$		0	1	2	0	1	0	2	1	2
$x_1^0 x_2^0$	[0,0]	1	1	1	1	1	1	1	1	1
$x_1^0 x_2^1$	[0,1]	0	1	2	0	1	0	2	1	2
$x_1^0 x_2^2$	[0,2]	0	1	1	0	1	0	1	1	1
$x_1^1 x_2^0$	[1,0]	0	0	0	1	1	2	1	2	2
$x_1^1 x_2^1$	[1,1]	0	0	0	0	1	0	2	2	1
$x_1^2 x_2^0$	[2,0]	0	0	0	1	1	1	1	1	1

Figure: $\mathcal{R}_{\mathbb{F}_3}(2, 2) = C_3(AG_2(\mathbb{F}_3)) = [9, 6, 3]_3$

$$\mathcal{B} = \{x_1^{i_1} x_2^{i_2} \mid 0 \leq i_k \leq 2, i_1 + i_2 \leq 2\}.$$

$$\mathcal{I} = \{(i_1, i_2) \mid i_k \in \mathbb{F}_3, 1 \leq k \leq 2, i_1 + i_2 \leq 2\}$$

3-PD-sets for $C_p(AG_2(\mathbb{F}_p))$

Result ([KMM08])

Let $\mathcal{D} = AG_{2,1}(\mathbb{F}_p)$, where p is a prime, the design of points and lines in the affine plane $AG_2(\mathbb{F}_p)$, and let $C = \mathcal{R}_{\mathbb{F}_p}(p-1, 2) = [p^2, \binom{p+1}{2}, p]_p$ be the p -ary code of \mathcal{D} . With information set

$$\mathcal{I} = \{(i_1, i_2) \mid i_k \in \mathbb{F}_p, 1 \leq k \leq 2, \sum_{k=1}^2 i_k \leq (p-1)\},$$

the group TZ , where T is the translation group and Z is the group of scalar matrices, is a 3-PD-set for C for $p \geq 7$, of size $p^2(p-1)$.

Proof: Let for $a \in \mathbb{F}_p, a \neq 0$ let $\delta_a = aI_{p^2}$. Thus $Z = \{\delta_a \mid a \in \mathbb{F}_p, a \neq 0\}$.
Let $H = TZ$.

A translation can take any three points to the triple $X = (0, 0)$,
 $P = (a, b)$, $Q = (c, d)$ where not all of a, b, c, d are 0 and $(a, b) \neq (c, d)$,
i.e. $a \neq c$ or $b \neq d$.

Assume that $a \neq c$ (the other case will follow similarly). We find maps in
 H that move this triple into the check set \mathcal{C} .

Since $a \neq c$, some element of Z will fix X and map P and Q into the pair
 $(a, b), (a + 1, d)$, for some a, b, d , where $a \leq p - 2$. For this new triple,
the translation $T(p - a - 2, p - 1)$ will map the triple into \mathcal{C} unless
 $a = p - 2$ or $b \in \{1, 2\}$ or $d = 1$.

Proof continued

If $a = p - 2 = -2$ then δ_{-1} will map the points into a triple with $a = 1, a + 1 = 2$, so we need only address the other exclusions. If $b = 1$ then $T(p - a - 2, p - 2)$ will do unless $a = -2$ or $a = -3$, or $d = 1$, or $d = 2$. If $a = -2, -3$ then use δ_{-1} as before; if $d = 1$ then $T(k, p - 2)$ for $k \notin \{0, 1, p - a, p - a - 1\}$; if $d = 2$ then $T(p - a - 2, p - 3)$ will work unless $a \in \{-2, -3, -4\}$, in which case we use δ_{-1} as before. Finally, for the case $d = 1$ and arbitrary b , $T(p - a - 2, p - 2)$ will work, unless $b = 1, 2$, which cases are covered above.

Finally consider the triple $X, P = (0, b), Q = (0, c), b, c \neq 0$. For this, the translation $T(p - 1, k)$, where $k \notin \{0, p - b, p - c\}$, will work.

All cases are covered. ■

Some other results (if time permits)

Points and lines in affine 3-space

Result ([KMM08])

Let \mathcal{D} be the 2 - $(p^3, p, 1)$ design $AG_{3,1}(\mathbb{F}_p)$ of points and lines in the affine space $AG_3(\mathbb{F}_p)$, where p is a prime, and $C = \mathcal{R}_{\mathbb{F}_p}(2(p-1), 3) = C_p(\mathcal{D})$. Then C is a $[p^3, \frac{1}{6}p(5p^2 + 1), p]_p$ code with information set

$$\mathcal{I} = \{(i_1, i_2, i_3) \mid i_k \in \mathbb{F}_p, 1 \leq k \leq 3, \sum_{k=1}^3 i_k \leq 2(p-1)\}.$$

Let T be the translation group, D the invertible diagonal matrices, and for each $d \in \mathbb{F}_p$ with $d \neq 0$, let δ_d be the associated dilatation.

Using \mathcal{I} , for $p \geq 5$, $T \cup T\delta_{\frac{p-1}{2}}$ is a 2-PD-set for C of size $2p^3$;
for $p \geq 7$, TD is a 3-PD-set for C of size $p^3(p-1)^3$.

Prime-order (desarguesian) planes

2- and 3-PD-sets exist for any information set ; 4-PD-sets exist for particular information sets;

Using a Moorhouse [Moo91] basis,

2-PD-sets of 37 elements for the $[p^2, \binom{p+1}{2}, p]_p$ codes of the desarguesian affine planes of any prime order p and

2-PD-sets of 43 elements for the $[p^2 + p + 1, \binom{p+1}{2} + 1, p + 1]_p$ codes of the desarguesian projective planes of any prime order p were constructed in [KMM05].

Also 3-PD-sets for the code and the dual code in the affine prime case of sizes $2p^2(p - 1)$ and p^2 , respectively, were found.

Adjacency matrices of Paley graphs

If n is a prime power with $n \equiv 1 \pmod{4}$, the **Paley graph**, $P(n)$, has \mathbb{F}_n as vertex set and two vertices x and y are adjacent if and only if $x - y$ is a non-zero square in \mathbb{F}_n .

The row span over a field \mathbb{F}_p of an adjacency matrix gives an interesting code (quadratic residue codes) if and only if p is a square in \mathbb{F}_n .

For $\sigma \in \text{Aut}(\mathbb{F}_n)$, $a, b \in \mathbb{F}_n$ with a a non-zero square, the set of maps $\tau_{a,b,\sigma} : x \mapsto ax^\sigma + b$ is $\text{Aut}(P_n)$.

For $n \geq 1697$ and prime or $n \geq 1849$ and a square, PD-sets cannot exist since the bound of Result 2 is bigger than the order of the group (using the square root bound for the minimum weight, and the actual minimum weight $q + 1$ when $n = q^2$ and q is a prime power).

Paley graphs

If n is prime, $n \equiv 1 \pmod{8}$,

$$C_p(P(n)) = [n, \frac{n-1}{2}, d]_p$$

where $d \geq \sqrt{n}$, (the square-root bound) for p any prime dividing $\frac{n-1}{4}$.

$C_p(P(n))$ has a 2-PD-set of size 6 by [KL04].

(The automorphism group is not 2-transitive.)

For the dual code a 2-PD-set of size 10 for all n was found.

(Further results in [Lim05].)

Hamming graphs

The **Hamming graph** $H^k(n, m)$ has vertex set R^n , where R is a set of size m , and x, y adjacent if $d(x, y) = k$.

These are regular graphs with valency $(m - 1)\binom{n}{k}$.

(E.g. $H^1(n, 2) = H(n, 2) = Q_n$, the n -cube.)

The **neighbourhood design** is a symmetric $1-(q^n, (q - 1)\binom{n}{k}, (q - 1)\binom{n}{k})$ design with incidence matrix an adjacency matrix for the graph.

All these graphs, designs and codes have automorphism group containing $T \times S_n$, where T is the translation group.

The design can have a bigger automorphism group than that of the graph: e.g. for the n -cube the design's automorphism group is $(E \times S_n) \wr S_2$, where E denotes the translations using even-weight vectors.

Adjacency matrices of Hamming graphs

The 2- and 3-PD-sets for codes from adjacency matrices of Hamming graphs:

- 1 For n even $C_2(H^1(n, 2)) = [2^n, 2^{n-1}, n]_2$ is self-dual and has a 3-PD-set of size $n2^n$ inside $T \times S_n$ (the group of the graph, acting imprimitively) [KS07, Fis07];
- 2 for $n \equiv 0 \pmod{4}$ $C_2(H^2(n, 2)) = [2^n, 2^{n-1}, d]_2$ ($8 \leq d \leq \binom{n}{2}$) is self-dual, not isomorphic to the case above, but same 3-PD-set, different information set, works [FKM09b];
- 3 For $n \geq 3$ $C_2(H^1(n, 3)) = [3^n, \frac{1}{2}(3^n - (-1)^n), 2n]_2$, (with dual code the span of the adjacency matrix with 1's on the diagonal) then 2-PD-sets of size 9 can be found that work for the code or the dual. (The lower bound is 4 or 7). (The automorphism group is primitive.) [FKM09a, FKM10] Also 3-PD-sets of size $2n3^n$.

Reed-Muller codes

These are the codes of the affine geometry designs $AG_{m,r}(\mathbb{F}_2)$ and the punctured codes are those of the projective geometry designs $PG_{m,r}(\mathbb{F}_2)$. Some results on these to obtain small s -PD sets for first order Reed-Muller codes $\mathcal{R}(1, m)$ can be found in [KV08, Sen09].

The first- and second-order Reed-Muller codes, $\mathcal{R}(1, m)$ and $\mathcal{R}(2, m)$, are binary codes with large minimum weight, being the codes of the affine geometry designs over \mathbb{F}_2 of points and $(m - 1)$ -flats or $(m - 2)$ -flats, respectively, and with the minimum words the incidence vectors of the blocks.

Reed-Muller codes

In [KMM] the following was proved, extending results in [Sen09]:

Result ([KMM] Theorem 1)

Let $V = \mathbb{F}_2^m$ and $C_i = \{v \mid v \in V, wt(v) = i\}$ for $0 \leq i \leq m$. Let $T(u)$ denote the translation of V by $u \in V$,

$$A_m = \{T(u) \mid u \in C_0 \cup C_1 \cup C_2 \cup C_m\}, \quad B_m = A_m \cup \{T(u) \mid u \in C_3\},$$

then

- 1 A_m is an $(m-1)$ -PD-set of size $\frac{1}{2}(m^2 + m + 4)$ for $\mathcal{R}(1, m)$ for $m \geq 5$ for the information set $C_0 \cup C_1$;
- 2 B_m is an $(m+1)$ -PD-set of size $\frac{1}{6}(m^3 + 5m + 12)$ for $\mathcal{R}(1, m)$ for $m \geq 6$ for the information set $C_0 \cup C_1$;
- 3 B_m is an $(m-3)$ -PD-set of size $\frac{1}{6}(m^3 + 5m + 12)$ for $\mathcal{R}(2, m)$ for $m \geq 8$ for the information set $C_0 \cup C_1 \cup C_2$.

Triangular graphs

For any n , the **triangular graph** $T(n)$ is the line graph of the complete graph K_n , and is strongly regular.

The vertices are the $\binom{n}{2}$ 2-sets, with two vertices being adjacent if they intersect: this is in the class of **uniform subset graphs**.

The row span over \mathbb{F}_2 of an adjacency matrix gives codes:

$[\frac{n(n-1)}{2}, n-1, n-1]_2$ for n odd and

$[\frac{n(n-1)}{2}, n-2, 2(n-2)]_2$ for n even

where $n \geq 5$. [HPvR99]

The automorphism group is, apart from $n = 5$, S_n acting naturally; PD-sets of size n for n odd and $n^2 - 2n + 2$ for n even are found in [KMR04b].

Triangular graphs

$$\mathcal{I} = \{P_1 = \{1, n\}, P_2 = \{2, n\}, \dots, P_{n-1} = \{n-1, n\}\}$$

Then for $n \geq 5$, with \mathcal{I} in first $n-1$ positions,

- 1 C is a $[\binom{n}{2}, n-1, n-1]_2$ code for n odd and, with \mathcal{I} as the information positions,

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\}$$

is a PD-set for C of n elements in S_n ;

- 2 C is a $[\binom{n}{2}, n-2, 2(n-2)]_2$ code for n even, and with \mathcal{I} excluding P_{n-1} as the information positions,

$$\mathcal{S} \cup \{[(i, n-1)(j, n)]^{\pm 1} \mid 1 \leq i, j \leq n-2\}$$

is a PD-set for C of $n^2 - 2n + 2$ elements in S_n .

Graphs on triples

If Ω is a set of size n , let $\mathcal{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of graphs $A_i(n)$, for $i = 0, 1, 2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets have intersection of size i . Properties of the binary codes of adjacency matrices of these graphs were found in [KMR04a]. Again S_n in its natural action acts as an automorphism group of the graphs and codes:

Result ([KMR06])

If C is the binary code in the case of adjacency matrix of $A_2(n)$, then the dual C^\perp is a $[(\binom{n}{3}), (\binom{n-1}{2}), n-2]_2$ code and a PD-set of size n^3 can be found by

(Similarly for the ternary codes of these graphs.)

W. Fish [Fis07] worked on binary codes from **uniform subset graphs** in general (odd graphs, Johnson graphs, Knesner graphs, etc.)

Rectangular lattice graph

Nested s -PD-sets:

Result ([Sen07])

If $C = C_2(L_2(m, n)) = C_2(L(K_{m,n}))$ (the rectangular lattice graph) for $2 \leq m < n$, then C is

- $[mn, m + n - 2, 2m]_2$ for $m + n$ even;
- $[mn, m + n - 1, m]_2$ for $m + n$ odd.

The set $\mathcal{I} = \{(i, n) | 1 \leq i \leq m\} \cup \{(m, i) | 1 \leq i \leq n - 1\}$ is an information set for $m + n$ odd, and $\mathcal{I} \setminus \{(1, n)\}$ is an information set for $m + n$ even.

The sets of automorphisms

- $S_s = \{((i, m), (i, n)) | 1 \leq i \leq 2s\} \cup \{id\}$ for $m + n$ odd;
- $S_s = \{((i, m), (j, n)) | 1 \leq i \leq m, 1 \leq j \leq s\} \cup \{id\}$ for $m + n$ even

are s -error correcting PD-sets for any $0 \leq s \leq t$ errors.

References



E. F. Assmus, Jr and J. D. Key.

Designs and their Codes.

Cambridge: Cambridge University Press, 1992.

Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).



W. Bosma, J. Cannon, and C. Playoust.

The Magma algebra system I: The user language.

J. Symb. Comp., 24, 3/4:235–265, 1997.



Aart Blokhuis and G. Eric Moorhouse.

Some p -ranks related to orthogonal spaces.

J. Algebraic Combin., 4:295–316, 1995.



J. Cannon, A. Steel, and G. White.

Linear codes over finite fields.

In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006.

V2.13, <http://magma.maths.usyd.edu.au/magma>.



Washiela Fish.

Codes from uniform subset graphs and cyclic products.

PhD thesis, University of the Western Cape, 2007.



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

Codes from the incidence matrices and line graphs of Hamming graphs $H^k(n, 2)$ for $k \geq 2$.

(Submitted).



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

Codes, designs and groups from the Hamming graphs.

J. Combin. Inform. System Sci., 34:169–182, 2009.

No.1 – 4.



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

Graphs, designs and codes related to the n -cube.

Discrete Math., 309:3255–3269, 2009.



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

Codes from the incidence matrices and line graphs of Hamming graphs.



D. Ghinelli and J. D. Key.

Codes from incidence matrices of Paley graphs.

In preparation.



D. M. Gordon.

Minimal permutation sets for decoding the binary Golay codes.

IEEE Trans. Inform. Theory, 28:541–543, 1982.



Willem H. Haemers, René Peeters, and Jeroen M. van Rijckevorsel.

Binary codes of strongly regular graphs.

Des. Codes Cryptogr., 17:187–209, 1999.



W. Cary Huffman.

Codes and groups.

In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998.

Volume 2, Part 2, Chapter 17.



J. D. Key and J. Limbupasiriporn.

Permutation decoding of codes from Paley graphs.

Congr. Numer., 170:143–155, 2004.



J. D. Key, T. P. McDonough, and V. C. Mavron.
Reed-Muller codes and permutation decoding.
Discrete Math. To appear.



J. D. Key, T. P. McDonough, and V. C. Mavron.
Partial permutation decoding for codes from finite planes.
European J. Combin., 26:665–682, 2005.



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



J. D. Key, T. P. McDonough, and V. C. Mavron.
Partial permutation decoding for codes from affine geometry designs.
J. Geom., 88:101–109, 2008.



J. D. Key, J. Moori, and B. G. Rodrigues.
Binary codes from graphs on triples.
Discrete Math., 282/1-3:171–182, 2004.

 J. D. Key, J. Moori, and B. G. Rodrigues.

Permutation decoding for binary codes from triangular graphs.
European J. Combin., 25:113–123, 2004.

 J. D. Key, J. Moori, and B. G. Rodrigues.

Binary codes from graphs on triples and permutation decoding.
Ars Combin., 79:11–19, 2006.


 J. D. Key and B. G. Rodrigues.

Codes associated with lattice graphs, and permutation decoding.
Submitted.

 J. D. Key and P. Seneviratne.

Permutation decoding for binary self-dual codes from the graph Q_n where n is even.

In T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko, editors,
Advances in Coding Theory and Cryptology, pages 152–159. World
Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007.
Series on Coding Theory and Cryptology, 2.

 J. D. Key and P. Seneviratne.

Permutation decoding of binary codes from lattice graphs.

Discrete Math., 308:2862–2867, 2008.



Hans-Joachim Kroll and Rita Vincenti.

PD-sets related to the codes of some classical varieties.

Discrete Math., 301:89–105, 2005.



Hans-Joachim Kroll and Rita Vincenti.

PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of $PG(5,2)$.

Discrete Math., 308:408–414, 2008.



J. Limbupasiriporn.

Partial permutation decoding for codes from designs and finite geometries.

PhD thesis, Clemson University, 2005.



F. J. MacWilliams.

Permutation decoding of systematic codes.

Bell System Tech. J., 43:485–505, 1964.



G. Eric Moorhouse.

Bruck nets, codes, and characters of loops.

Des. Codes Cryptogr., 1:7–29, 1991.



F. J. MacWilliams and N. J. A. Sloane.

The Theory of Error-Correcting Codes.

Amsterdam: North-Holland, 1983.



J. Schönheim.

On coverings.

Pacific J. Math., 14:1405–1411, 1964.



Padmapani Seneviratne.

Permutation decoding of codes from graphs and designs.

PhD thesis, Clemson University, 2007.



P. Seneviratne.

Partial permutation decoding for the first-order Reed-Muller codes.

Discrete Math., 309:1967–1970, 2009.



Vladimir D. Tonchev.

Combinatorial Configurations, Designs, Codes, Graphs.

Pitman Monographs and Surveys in Pure and Applied Mathematics,
No. 40. New York: Longman, 1988.

Translated from the Bulgarian by Robert A. Melter.



J. Wolfmann.

A permutation decoding of the $(24,12,8)$ Golay code.

IEEE Trans. Inform. Theory, 29:748–750, 1983.

THANK FOR YOUR ATTENTION

