Permutation decoding for codes from designs and graphs

J. D. Key

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

25 June 2008
Costermano

Abstract

The method of permutation decoding was first developed by MacWilliams [Mac64] in the early 60's and 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 specifed properties.

This talk will describe some recent developments in finding PD-sets for codes defined through the row-span over finite fields of incidence matrices of designs or adjacency matrices 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.

Coding theory terminology

- A **linear code** is a subspace of a finite-dimensional vector space over a finite field. (All codes are linear in this talk.)
- The **weight** of a vector 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 the code is a $k \times n$ matrix made up of a basis for C.
- The **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n | (v,c) = 0 \text{ for all } c \in C\}$.

Coding theory terminology continued

- A **check** matrix for C is a generator matrix H for $C^\perp$.
- Two linear codes of the same length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.
- An **automorphism** of a code C is an isomorphism from C to C.
- Any code is isomorphic to a code with generator matrix in **standard form**, i.e. the form $[I_k \,|\, A]$; 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

Definition

If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then 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 $\mathcal{C}$.
[Huf98, Mac64, MS83]

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 $\mathcal{C}$. [KMM05, KV05]

Specifically, if $\mathcal{I} = \{1, \ldots, k\}$ are the information positions and $\mathcal{C} = \{k+1, \ldots, n\}$ the check positions, then every s-tuple from $\{1, \ldots, n\}$ can be moved by some element of $\mathcal{S}$ into $\mathcal{C}$.

Permutation decoding

Definition

If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then 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 $\mathcal{C}$.
[Huf98, Mac64, MS83]

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 $\mathcal{C}$. [KMM05, KV05]

Specifically, if $\mathcal{I} = \{1, \ldots, k\}$ are the information positions and $\mathcal{C} = \{k+1, \ldots, n\}$ the check positions, then every s-tuple from $\{1, \ldots, n\}$ 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:
$\mathcal{S}=\{g_1,\ldots,g_m\}$ 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 $i=1,\ldots,m$, 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 $u=u_1u_2\ldots u_k$ 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 the weight of the syndrome Hy^T of y is $\leq t$.

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

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

(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: 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]).

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.

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] 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.

Classes of codes having s-PD-sets

- If $\mathrm{Aut}(C)$ is k-transitive then $\mathrm{Aut}(C)$ itself is a k-PD-set, in which case we attempt to find smaller sets;
- existence of a k-PD-set is not invariant under code isomorphism;
- codes from the row span over a finite field $\mathbb{F}_p$ of an incidence matrix of a design or geometry $\mathcal{D}$ or from an adjacency matrix of a graph Γ, written $C_p(\mathcal{D})$ or $C_p(\Gamma)$, respectively;
- using Result 2 it follows that many classes of designs and graphs where the minimum-weight and automorphism group are known, cannot have PD-sets for full error-correction for length beyond some bound; for these we look for s-PD-sets with $2 \leq s < \lfloor \frac{d-1}{2} \rfloor$: e.g. finite planes, Paley graphs;
- for some classes of regular and semi-regular graphs with large automorphism groups, PD-sets exist for all lengths: e.g. binary codes of triangular graphs, lattice graphs, line graphs of complete multi-partite graphs.

Some infinite classes of codes having PD-sets

In all of these, suitable information sets had to be found.

1. **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
$[\frac{n(n-1)}{2}, n-2, 2(n-1)]_2$ for n even
where $n \geq 5$. [Hae99]
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].

Specifically, if

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

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

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

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

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

2. Graphs on triples

Define three graphs with vertex set the subsets of size three of a set of size n and adjacency according to the size of the intersection of the 3-subsets. Properties of these codes are in [KMR04a]. S_n in its natural action is the automorphism group.

If C is the binary code in the case of adjacency if the 3-subsets intersect in two elements, 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 [KMR06]. (Similarly for the ternary codes of these graphs.)

W. Fish (Cape Town) is working on binary codes from uniform subset graphs in general (odd graphs, Johnson graphs, Knesner graphs, etc.)

3. Lattice graphs

The (square) lattice graph $L_2(n)$ is the line graph of the complete bipartite graph $K_{n,n}$, and is strongly regular.
The binary code of $L_2(n)$ is $[n^2, 2(n-1), 2(n-1)]_2$ for $n \geq 5$ with $S_n \wr S_2$ as automorphism group.
PD-sets of size n^2 in $S_n \times S_n$ were found in [KS08].

A similar result holds for the (rectangular) lattice graph $L_2(m,n)$, $m < n$: the codes are
$[mn, m+n-2, 2m]_2$ for $m+n$ even,
$[mn, m+n-1, m]_2$ for $m+n$ odd.
PD-sets of size m^2+1 and $m+n$, respectively, in $S_m \times S_n$ were found in [KS06].

Similarly for the line graph $L_m(n)$ of the complete multipartite graphs $K_{n,\ldots,n}$, with automorphism group $S_n \wr S_m$. [KS07a].

Time complexity

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

$$S_0 < S_1 \ldots < S_t$$

and arrange the PD-set S in this order:

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

(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 information set

$$\{(i,n)|2 \leq i \leq n-1\} \cup \{(n,i)|1 \leq i \leq n\},$$

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

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

is a k-PD-set.
((n,n) is the identity permutation in S_n.)

Thus ordering the elements of the PD-set as

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

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.

Result

[Sen07] If $C = C_2(L_2(m,n))$ (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* $\mathcal{I} \backslash \{(1,n)\}$ *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.*

A study of the complexity of the algorithm for some algebraic geometry codes is give in [Joy05].

Some infinite classes of codes having only s-PD-sets

1. **Finite planes**

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

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.

Information sets for 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* $\mathbb{F}_q = \{\alpha_0, \ldots, \alpha_{q-1}\}$. *Then*

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

is an information set for $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$.
If $q = p$ *is a prime,*

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

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

Examples to illustrate the theorem

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

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

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

Result

[KMM06] If $C = C_p(PG_{m,m-1}(\mathbb{F}_p))$, where p is a prime and $m \geq 2$, then, using homogeneous coordinates, the incidence vectors of the set

$$\{(1, a_1, \ldots, a_m)' \mid a_i \in \mathbb{F}_p, \sum_{i=1}^{m} a_i \leq p-1\} \cup \{(0, \ldots, 0, 1)'\}$$

of hyperplanes form a basis for C.
Similarly, a basis of hyperplanes for $C_p(AG_{m,m-1}(\mathbb{F}_p))$ for $m \geq 2$, p prime is the set of incidence vectors of the hyperplanes with equation

$$\sum_{i=1}^{m} a_i X_i = p-1 \text{ with } \sum_{i=1}^{m} a_i \leq p-1,$$

where $a_i \in \mathbb{F}_p$ for $1 \leq i \leq m$, and not all the a_i are 0, along with the hyperplane with equation $X_m = 0$.

Example

A basis of minimum-weight vectors for $C_3(PG_{2,1}(\mathbb{F}_3))$.

	0 0 1	1 0 0	1 0 1	1 0 2	1 1 0	1 1 1	1 2 0	1 1 2	1 2 1	1 2 2	0 1 0	0 1 1	0 1 2
$(0,0,1)'$	0	1	0	0	1	0	1	0	0	0	1	0	0
$(1,0,0)'$	1	0	0	0	0	0	0	0	0	0	1	1	1
$(1,0,1)'$	0	0	0	1	0	0	0	1	0	1	1	0	0
$(1,0,2)'$	0	0	1	0	0	1	0	0	1	0	1	0	0
$(1,1,0)'$	1	0	0	0	0	0	1	0	1	1	0	0	0
$(1,1,1)'$	0	0	0	1	0	1	1	0	0	0	0	0	1
$(1,2,0)'$	1	0	0	0	1	1	0	1	0	0	0	0	0

Figure: $C_3(PG_{2,1}(\mathbb{F}_3))$

Example

A basis of minimum-weight vectors for $\mathcal{R}_{\mathbb{F}_3}(2,2) = C_3(AG_{2,1}(\mathbb{F}_3))$.

	0	0	0	1	1	2	1	2	2
	0	1	2	0	1	0	2	1	2
$X_2 = 0$	1	0	0	1	0	1	0	0	0
$X_2 = 2$	0	0	1	0	0	0	1	0	1
$X_2 = 1$	0	1	0	0	1	0	0	1	0
$X_1 = 2$	0	0	0	0	0	1	0	1	1
$X_1 + X_2 = 2$	0	0	1	0	1	1	0	0	0
$2X_1 = 2$	0	0	0	1	1	0	1	0	0

Figure: $\mathcal{R}_{\mathbb{F}_3}(2,2) = C_3(AG_{2,1}(\mathbb{F}_3))$

Compare with the generator matrix using the polynomial basis 1.

Partial permutation decoding

1.**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.

2.Points and lines in 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 $p^3(p-1)^3$.

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

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).

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].)

4. Hamming graphs

The Hamming graph $H^k(n,q)$ has vertex set $\mathbb{F}_q^n$, x,y adjacent if $\mathrm{wt}(x-y)=k$.

These are regular graphs with valency $(q-1)\binom{n}{k}$.
(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 $T \rtimes S_n$, 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 $(E \rtimes S_n) \wr S_2$, where E denotes the translations using even-weight vectors.

The 2- and 3-PD-sets:

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 $T \rtimes S_n$ (the group of the graph, acting imprimitively) [KS07b, 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 [FKMb];
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.) [FKMa] Also 3-PD-sets of size $2n3^n$.

5. **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 [KV, Sen].

For the designs of points and hyperplanes, from [KMM06], the translation group (of size 2^m) is an s-PD-set for $\mathcal{R}(1,m)$ for $s = \lfloor \frac{2^m-1}{m+1} \rfloor$ for $m \geq 4$ and the Singer group (of size $2^{m+1}-1$) is an s-PD-set for $\mathcal{R}(1,m+1)^*$ for $s = \lfloor \frac{2^{m+1}-1}{m+2} \rfloor$.

References

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, designs and groups from the Hamming graphs.
In preparation.

References

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

D. M. Gordon.
Minimal permutation sets for decoding the binary Golay codes.
IEEE Trans. Inform. Theory, 28:541–543, 1982.

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.

David Joyner.
Conjectural permutation decoding of some AG codes.
ACM SIGSAM Bulletin, 39, 2005.
No.1, March.

References

- 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.
  Partial permutation decoding of 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 of codes from finite geometries.
  Finite Fields Appl., 12:232–247, 2006.

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

References

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 P. Seneviratne.
Binary codes from rectangular lattice graphs and permutation decoding.
European J. Combin., 28:121–126, 2006.

References

J. D. Key and P. Seneviratne.
Codes from the line graphs of complete multipartite graphs and PD-sets.
Discrete Math., 307:2217–2225, 2007.

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.

References

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)).
Submitted 2005.

Hans-Joachim Kroll and Rita Vincenti.
PD-sets related to the codes of some classical varieties.
Discrete Math., 301:89–105, 2005.

J. Limbupasiriporn.
Partial permutation decoding for codes from designs and finite geometries.
PhD thesis, Clemson University, 2005.

G. Eric Moorhouse.
Bruck nets, codes, and characters of loops.
Des. Codes Cryptogr., 1:7–29, 1991.

References

J. Schönheim.
On coverings.
Pacific J. Math., 14:1405–1411, 1964.

Padmapani Seneviratne.
Partial permutation decoding for the first-order Reed-Muller codes.
Disc. Math., To appear.

Padmapani Seneviratne.
Permutation decoding of codes from graphs and designs.
PhD thesis, Clemson University, 2007.

J. Wolfmann.
A permutation decoding of the (24,12,8) Golay code.
IEEE Trans. Inform. Theory, *29:748–750, 1983.*

References

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.

F. J. MacWilliams.
Permutation decoding of systematic codes.
Bell System Tech. J., 43:485–505, 1964.

F. J. MacWilliams and N. J. A. Sloane.
The Theory of Error-Correcting Codes.
Amsterdam: North-Holland, 1983.