Department of Mathematical Sciences, Clemson University

http://www.ces.clemson.edu/ keyj/

Some recent developments in permutation decoding

J. D. Key

keyj@ces.clemson.edu

Abstract

The method of permutation decoding was first developed by MacWilliams 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, since 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.

May 8, 2006

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. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$.
- A **check** matrix for C is a generator matrix H for $C^\perp$.

Coding theory terminology continued

- 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

Permutation decoding was first developed by Jessie MacWilliams [Mac64] following also Prange [Pra62]. It can be used when a code has sufficiently many automorphisms to ensure the existence of a set of automorphisms called a PD-set. Early work was mostly on cyclic codes and the Golay codes.

We extend the definition of PD-sets to s-PD-sets for s-error-correction [KMM05]:

Definition 1 *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 $\mathcal{C}$.*

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 $\mathcal{C}$.

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 q-ary t-error-correcting $[n,k,d]_q$ code; $d = 2t+1$ or $2t+2$.

$k \times n$ generator matrix for C: $G = [I_k|A]$.
Any k-tuple v is encoded as vG. The first k columns are the information symbols, the last $n-k$ are check symbols.

$(n-k) \times n$ check matrix for C: $H = [-A^T|I_{n-k}]$.
$\mathcal{S} = \{g_1, \ldots, g_m\}$ 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;

Algorithm for permutation decoding

C is a q-ary t-error-correcting $[n, k, d]_q$ code; $d = 2t + 1$ or $2t + 2$.

$k \times n$ generator matrix for C: $G = [I_k | A]$.
Any k-tuple v is encoded as vG. The first k columns are the information symbols, the last $n - k$ are check symbols.

$(n - k) \times n$ check matrix for C: $H = [-A^T | I_{n-k}]$.
$\mathcal{S} = \{g_1, \ldots, g_m\}$ 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 $u = u_1 u_2 \ldots u_k$ are the information symbols of yg_i, compute the codeword $c = uG$;

Algorithm for permutation decoding

C is a q-ary t-error-correcting $[n, k, d]_q$ code; $d = 2t + 1$ or $2t + 2$.

$k \times n$ generator matrix for C: $G = [I_k | A]$.
Any k-tuple v is encoded as vG. The first k columns are the information symbols, the last $n - k$ are check symbols.

$(n - k) \times n$ check matrix for C: $H = [-A^T | I_{n-k}]$.
$\mathcal{S} = \{g_1, \ldots, g_m\}$ 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 $u = u_1 u_2 \ldots u_k$ are the information symbols of yg_i, compute the codeword $c = uG$;
- decode y as cg_i^{-1}.

Why permutation decoding works

Result 1 *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 redundancy positions. Let $y = c+e$ be a vector, 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 $\leq t$.*

Time complexity

A simple argument yields that the worst-case time complexity for the decoding algorithm using an s-PD-set of size m on a code of length n and dimension k is $\mathcal{O}(nkm)$.

So small PD-sets are desirable. Further, 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 m-PD-set S_m for each $0 \leq m \leq t$ 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 $S_0 = \{id\}$).

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

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

(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]).

Design theory background

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. Taking $t \geq 1$, the number of blocks incident with a given point is constant for the design, called the replication number for $\mathcal{D}$. If $\mathcal{B} = b$ then $bk = vr$.

E.g. A 2-$(n^2 + n + 1, n + 1, 1)$ is a projective plane of order n, where $n = p^e$ is a prime power (in all known cases); a $2 - (16, 6, 2)$ is a biplane.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F, i.e. the row span over F of a $b \times v$ incidence matrix, a 0-1 matrix with k 1's in every row and r 1's in every column: see [AK92, AK96].

Similarly, the code of a regular undirected graph Γ over a finite field F is the row span over F of an adjacency matrix for Γ. This matrix has k 1's in every row and column, where k is the valency of the graph.

Finding PD-sets

First we need an information set. These are not known in general; further different information sets will yield different possibilities for PD-sets.

For symmetric designs (e.g. 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. Recently a convenient information set for the designs of points and hyperplanes of prime order was found in [KMM06] (I'll get back to this.)

NOTE: Magma [BC94] 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 of an incidence matrix of a design or geometry, or from an adjacency matrix of a graph;
- 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 $n \geq 5$.

The automorphism group is S_n acting naturally (apart from $n = 5$) and get PD-sets of size n for n odd and $n^2 - 2n + 2$ for n even, by [KMR04b].

(The computational complexity of the decoding by this method may be quite low, of the order $n^{1.5}$ if the elements of the PD-set are appropriately ordered.)

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]. Again S_n in its natural action is the automorphism group. The ternary codes of these graphs are also of interest.

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 n^3 can be found by [KMR].

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 row span over $\mathbb{F}_2$ of an adjacency matrix gives codes: $[n^2, 2(n-1), 2(n-1)]_2$ for $n \geq 5$ with $S_n \wr S_2$ as automorphism group, and PD-sets of size n^2 in $S_n \times S_n$ were found in [KSc].

(The lower bound from Result 2 is $O(n)$.)

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 $S_m \times S_n$ can be found. [KSa].

More generally for the line graphs of multi-partite graphs, with automorphism group $S_{n_1} \times S_{n_2} \times \ldots \times S_{n_m}$: [KSb].

Complexity of permutation decoding

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

Proposition 1 *For the* $[n^2, 2(n-1), 2(n-1)]_2$ *code from the row span of an adjacency matrix of 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, where* (n,n) *denotes 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.

Proposition 2 *If C is the binary code formed by the row space over $\mathbb{F}_2$ of an adjacency matrix for the rectangular lattice graph $L_2(m,n)$ 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 only having partial 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 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, for some r, in projective or affine space, have GRM codes and the 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 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. For example, in the projective desarguesian case when:

$q = p$ 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

$$\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid 0 \le i_k \le q-1, \text{ for } 1 \le k \le m, \sum_{k=1}^{m} i_k \le \rho \rangle.$$

is the **ρ^{th}-order generalized Reed-Muller code** $\mathcal{R}_{\mathbb{F}_q}(\rho, m)$, of length q^m over the field $\mathbb{F}_q$. In [KMM06] we found information sets for these codes:

Theorem 3 *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*

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

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

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

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
$x_1^0 x_2^0 = 1$	[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 1: $\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \mathcal{R}_{\mathbb{F}_3}(2,2) = [9,6,3]_3$

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

Proposition 4 *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

$$\sum_{i=1}^{m} a_i X_i = p-1$$

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	1	1	1	1	1	1	1	1	1	0	0	0
	0	0	0	0	1	1	2	1	2	2	1	1	1
	1	0	1	2	0	1	0	2	1	2	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 2: $C_3(PG_{2,1}(\mathbb{F}_3))$

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	0 2	1 0	1 1	2 0	1 2	2 1	2 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 3: $\mathcal{R}_{\mathbb{F}_3}(2,2) = C_3(AG_{2,1}(\mathbb{F}_3))$

Compare with the generator matrix using the polynomial basis 1.

Small 2-PD-sets in prime-order planes

2-PD-sets exist for any information set (since the group is 2-transitive);
for prime order, 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.

Other orders q and other codes from geometries yield similar results.

2. Points and lines in 3-space

Theorem 5 *[KMM] 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 let $C = \mathcal{R}_{\mathbb{F}_p}(2(p-1), 3)$ be the p-ary code of $\mathcal{D}$. Then C is a $[p^3, \frac{1}{6}p(5p^2+1), p]_p$ code with information set*

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

Let T is the translation group, D the group of invertible diagonal 3×3 matrices, and Z the group of scalar matrices, and, for each $d \in \mathbb{F}_p$ with $d \neq 0$, let δ_d be the associated dilatation. Using this information set, for $p \ge 5$ there exists $d \in \mathbb{F}_p^*$ such that C has an 2-PD-set of the form $T \cup T\delta_d$ of size $2p^3$, and for $p \ge 7$ TD is a 3-PD-set for C of size $p^3(p-1)^3$. (In fact $d = \frac{p-1}{2}$ will be suitable for the 2-PD-set.)

Note: These codes have high rate $\ge .83$.

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 any $\sigma \in Aut(\mathbb{F}_n)$ and $a, b \in \mathbb{F}_n$ with a a non-zero square, the group of maps $\tau_{a,b,\sigma} : x \mapsto ax^{\sigma} + b$ is the automorphism group of the code, and 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).

For the case where n is prime and $n \equiv 1 \pmod 8$, the code of $P(n)$ over $\mathbb{F}_p$ is $C = [n, \frac{n-1}{2}, d]_p$ where $d \geq \sqrt{n}$,
(the square-root bound) for p any prime dividing $\frac{n-1}{4}$.

C has a 2-PD-set of size 6 by [KL04]. (The automorphism group is not 2-transitive.)

For the dual code in this case, a 2-PD-set of size 10 for all n was found. Further results in [Lim05].

References

[AK92] 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).

[AK96] E. F. Assmus, Jr. and J. D. Key. Designs and codes: an update. *Des. Codes Cryptogr.*, 9:7–27, 1996.

[BC94] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://magma.maths.usyd.edu.au/magma/.

[BM95] Aart Blokhuis and G. Eric Moorhouse. Some p-ranks related to orthogonal spaces. *J. Algebraic Combin.*, 4:295–316, 1995.

[Gor82] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[Huf98] 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.

[Joy05] David Joyner. Conjectural permutation decoding of some AG codes. *ACM SIGSAM Bulletin*, 39, 2005. No.1, March.

[KL04] J. D. Key and J. Limbupasiriporn. Permutation decoding of codes from Paley graphs. *Congr. Numer.*, 170:143–155, 2004.

[KMM] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from affine geometry designs. Submitted.

[KMM05] 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.

[KMM06] 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.

[KMR] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples and permutation decoding. *Ars Combin.* To appear.

[KMR04a] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples. *Discrete Math.*, 282/1-3:171–182, 2004.

[KMR04b] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding for binary codes from triangular graphs. *European J. Combin.*, 25:113–123, 2004.

[KSa] J. D. Key and P. Seneviratne. Binary codes from rectangular lattice graphs and permutation decoding. *European J. Combin.*,To appear.

[KSb] J. D. Key and P. Seneviratne. Codes from the line graphs of complete multipartite graphs and PD-sets. Submitted.

[KSc] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.* (Special issue dedicated to J. Seberry), To appear.

[Lim05] J. Limbupasiriporn. *Partial permutation decoding for codes from designs and finite geometries*. PhD thesis, Clemson University, 2005.

[Mac64] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[Moo91] G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Des. Codes Cryptogr.*, 1:7–29, 1991.

[Pra62] E. Prange. The use of information sets in decoding cyclic codes. *IRE Trans.*, IT-8:5–9, 1962.

[Sch64] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[Wol83] J. Wolfmann. A permutation decoding of the (24,12,8) Golay code. *IEEE Trans. Inform. Theory*, 29:748–750, 1983.