Department of Mathematical Sciences, Clemson University

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

Some recent results in permutation decoding

J. D. Key

keyj@ces.clemson.edu

Introduction

Permutation decoding was first developed by Jessie MacWilliams [10] in the early 60's. It can be used when a code has sufficiently many automorphisms to ensure the existence of a set of automorphisms called a PD-set:

Definition 1 *A PD-set for a code is a set $\mathcal{S}$ of automorphisms of the code which is such that, if the code can correct t errors, then every possible error vector of weight t or less can be moved by some member of $\mathcal{S}$ out of the information positions.*

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

Such a set will fully use the error-correction potential of the code, but that such a set exists at all is clearly not always true, and existence is not invariant under code equivalence. There is a bound on the minimum size that the set $\mathcal{S}$ may have.

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: $H = [-A^T|I_{n-k}]$.

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

$\mathcal{S} = \{g_1, \ldots, g_s\}$ is a PD-set for C.

- For $i = 1, \ldots, s$, 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 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 $\leq t$.*

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 [4], using a result of Schönheim [12]:

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 [5].)

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 [4] and Wolfmann [13]).

Magma results

Some computational examples using Magma [2]:

1. for C the $[28, 21, 4]_2$ code of the hermitian unital 2-(28,4,1) has $|S| \geq 4$; Aut(C) is $\mathrm{Sp}_6(2)$ and a PD-set of four elements can be found;
2. $C^{\perp}$, for C as above, is a $[28, 7, 12]_2$; here $|S| \geq 10$; found a PD-set of 30 elements;
3. C the $[31, 16, 6]_5$ code with $PGL_3(F_5)$ acting (cyclic code), the bound is 7, and a set of 14, inside a cyclic group of order 31 was found;
4. the dual of the above is a $[31, 15, 10]_5$ code, self-orthogonal, the bound is 28, and the normalizer of a Sylow 31-subgroup has order 93. One such group was found to be a PD-set.
5. C the $[57, 29, 8]_7$ code with $PGL_3(F_7)$ acting (cyclic code), the bound is 15, and a set of 43 was found inside the normalizer (of order 171) of a regular cyclic group of order 57, and one of size 54 was found inside a regular cyclic group of order 57.

Single error

Correcting a single error is, in fact, simply done by using syndrome decoding, since in that case multiples of the columns of the check matrix will give the possible syndromes. Thus the syndrome of the received vector need only be compared with the columns of the check matrix, by looking for a multiple.

PD-sets for cyclic codes

MacWilliams [10] developed a theory for finding PD-sets for cyclic codes.

An $[n, k, d]_q$ C is cyclic if whenever $c = c_1 c_2 \dots c_n \in C$ then every cyclic shift of c is in C. Thus the mapping $T \in S_n$ defined by

$$T : i \mapsto i + 1$$

for $i \in \{1, 2, \dots n\}$, is in the automorphism group of C, and $T^n = 1$. 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 T^j for some j will move the sequence of zeros into the information positions, and thus all the errors will occur in the check positions.

Thus the elements of $\langle T \rangle$ will be a PD-set for C if $k < \frac{n}{t}$.

If also $(n, q) = 1$ (i.e. the greatest common divisor of q and n is 1) then the map

$$U : i \mapsto qi$$

is also an automorphism. Such a map can improve on the largest gap between errors, i.e. on the longest sequence of zeros between errors.

Thus the group $H = \langle T, U \rangle$ may contain a PD-set for the code.

Previous work on finding PD-sets for special types of codes includes Wolfmann [13] for Golay codes and Chabanne [3] for abelian codes. For the latter, the method uses Gröbner bases.

We try codes and designs.

Some examples of PD-sets for codes from designs and graphs

1. Triangular graphs

For any n, the triangular graph $T(n)$ is the line graph of the complete graph K_n, i.e. the vertices are the 2-subsets $\mathcal{P}$ of $\Omega = \{1, 2, \ldots, n\}$ and vertices $\{a, b\}$ and $\{c, d\}$ in $\mathcal{P}$ are adjacent if they have one letter from Ω in common. Thus the valency is $2(n-1)$.

If A is an adjacency matrix for $T(n)$ the row span of A over the field $GF(2)$ of order 2 forms a binary code with parameters

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

for n odd and

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

for n even, taking $n \geq 5$ to avoid trivial cases.

Information positions

Order the points as follows:

$$P_1 = \{1, n\}, P_2 = \{2, n\}, \ldots, P_{n-1} = \{n-1, n\},$$

first, followed by the set

$$P_n = \{1, 2\}, P_{n+1} = \{1, 3\}, \ldots,$$

$$P_{2n-2} = \{2, 3\}, \ldots, P_{\binom{n}{2}} = \{n-2, n-1\}.$$

It can be shown that a generator matrix for C in standard form can be found with the first $n-1$ coordinates the information symbols for n odd, and the first $n-2$ for n even.

PD-sets for the codes

Result 3 (Key, Moori & Rodrigues [7]) *Using for information symbols the points described above, the following sets of permutations in S_n in the natural action on the points $\mathcal{P}$, are PD-sets for the binary code C of the triangular graph $T(n)$.*

1. *For $n \geq 5$ odd,*

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

is a PD-set of n elements.

2. *For $n \geq 6$ and even,*

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

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

is a PD-set of $n^2 - 2n + 2$ elements.

(Recall that $C(n)$ corrects $\frac{n-3}{2}$ errors if n is odd, and $n-3$ errors if n is even.)

Lower Bound

If C is the binary code of the triangular graph $T(n)$ then:

- For $n \geq 5$ odd, the lower bound for the size of a PD-set for C is $\frac{n-1}{2}$;
- For $n \geq 18$ and even, the following formula appears to hold: writing $n = 2k + 18$, $k = \frac{n-18}{2} \pmod 6 \in \{0, 1, 2, 3, 4, 5\}$, $k \geq 0$, the bound for n is

$$n - 2 + 10 \left\lfloor \frac{n-6}{12} \right\rfloor + k + \left\lfloor \frac{k}{2} \right\rfloor .$$

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. The codes are low density parity check (LDPC) codes.

2. Lattice graphs $L_2(n)$

The **lattice graph** $L_2(n)$ has vertex set the set $\mathcal{P}$ of ordered pairs $\{(i,j) \mid 1 \leq i,j \leq n\}$, where two pairs are adjacent if and only if they have a common coordinate. $L_2(n)$ is strongly regular of type $(n^2, 2(n-1), n-2, 2)$.

Result 4 *For $n \geq 5$, the automorphism group of the lattice graph $L_2(n)$ is $S_n \wr S_2$, the wreath product of S_n with S_2. The binary code formed by the row space over F_2 of an adjacency matrix for $L_2(n)$ is a $[n^2, 2(n-1), 2(n-1)]_2$ code with $S_n \wr S_2$ acting as an automorphism group.*

PD-sets for the codes

Result 5 (Key & Seneviratne [9]) *For $n \geq 5$, let C be the $[n^2, 2(n-1), 2(n-1)]_2$ binary code from the row span of an adjacency matrix for the lattice graph $L_2(n)$. Then a PD-set of n^2 elements can be found for C. Using the $2(n-1)$ points (ordered pairs)*

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

as information symbols, the set

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

of permutations in $S_n \times S_n$, in the natural action on the points (ordered pairs), forms a PD-set of size n^2 for C.

Here (n, n) denotes the identity element of S_n.

Recall that the code corrects $t = n - 2$ errors.

Proof of Result 5

Denote the information symbols by $\mathcal{I}$. Now C can correct $t = n-2$ errors, so we need to show that every set of $s \leq t$ points can be moved by some element of $\mathcal{S}$ into the check positions $\mathcal{E}$. Let

$$\mathcal{T} = \{(a_1, b_1), (a_2, b_2), \ldots, (a_s, b_s)\}$$

be a set of $s \leq t = n-2$ points of $\mathcal{P}$.

Let $\Omega_1 = \{a_1, a_2, \ldots, a_s\}$ and $\Omega_2 = \{b_1, b_2, \ldots, b_s\}$.

Then $|\Omega_i| \leq n-2$ for $i = 1, 2$ and thus we can find $k \neq n$ and $l \neq n$ such that $k \notin \Omega_1$ and $l \notin \Omega_2$. Then

$$g = ((k, n), (l, n)) \in S_n \times S_n$$

will satisfy $\mathcal{T}^g \subseteq \mathcal{E}$. Thus $\mathcal{S}$ forms a PD-set for the code. ■

Lower bound

Using Magma [2] we found that the following formulae for the lower bound (Result 2) appear to hold, showing that the bound is linear in n:

- for n odd:

$$n \equiv 9 \pmod{12},\ n \geq 21 \quad : \quad \frac{1}{2}(5n-11) - 2\lfloor \frac{n-3}{4} \rfloor - \lceil \frac{n-5}{6} \rceil = \frac{1}{6}(11n-15);$$

$$n \not\equiv 9 \pmod{12},\ n \geq 29 \quad : \quad \frac{1}{2}(5n-11) - 2\lfloor \frac{n-3}{4} \rfloor - \lfloor \frac{n-5}{6} \rfloor;$$

- for $n \geq 12$ even:

$$2n - 3 - \lceil \frac{n-2}{4} \rceil + \lfloor \frac{n-6}{12} \rfloor.$$

3. Lattice graphs $L_2(m,n)$, $m < n$

The **lattice graph** $L_2(m,n)$ for $m < n$ has vertex set the set $\mathcal{P}$ of ordered pairs $\{(i,j) \mid 1 \le i \le m, 1 \le j \le n\}$, where two pairs are adjacent if and only if they have a common coordinate. It is a regular graph of valency $m+n-2$.

Result 6 *For $5 \le m \le n$ the automorphism group of the lattice graph $L_2(m,n)$ contains $S_m \times S_n$. If C is the binary code formed by the row space over F_2 of an adjacency matrix for $L_2(m,n)$ for $m < n$, then C is*

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

PD-sets for the codes

Result 7 *Let C be the binary code of the lattice graph $L_2(m,n)$ for $5 \leq m < n$,*

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

and

$$\mathcal{S} = \{((i,m),(j,n)) \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}.$$

Then $\mathcal{S}$ is a PD-set of mn elements for C using $\mathcal{I}$ as information symbols for $m+n$ odd, and $\mathcal{I} \setminus \{(1,n)\}$ for $m+n$ even.

4. Graphs on triples

Let Ω a set of size $n \geq 7$. Let $\mathcal{P} = \Omega^{\{3\}}$ denote the set of all 3-element subsets of Ω. Define three undirected graphs $A_i(n)$ where $i = 0, 1, 2$ with vertex set $\mathcal{P}$ as follows: two vertices are adjacent in $A_i(n)$ if as 3-element subsets they have exactly i elements of Ω in common.

The valency of these graphs is given by:

- $\binom{n-3}{3}$ for $A_0(n)$;
- $3\binom{n-3}{2}$ for $A_1(n)$;
- $3(n-3)$ for $A_2(n)$.

Result 8 (Key, Moori & Rodrigues [6]) *Let Ω be a set of size n, where $n \geq 7$. Let $\mathcal{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of the three graphs $A_i(n)$, for $i = 0, 1, 2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in zero, one or two elements, respectively. Let $C_i(n)$ denote the code formed from the row span over F_2 of an adjacency matrix for $A_i(n)$. Then*

1. $n \equiv 0 \pmod 4$:
   a) $C_2(n) = F_2^{\mathcal{P}}$;
   b) $C_0(n) = C_1(n)$ is a $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ code, and $C_0(n)^\perp$ is a $[\binom{n}{3}, n, \binom{n-1}{2}]_2$ code;
   c) $C_i(n) \cap C_i(n)^\perp = \{0\}$ for $i = 0, 1, 2$;
2. $n \equiv 2 \pmod 4$:
   $C_i(n) = F_2^{\mathcal{P}}$ for $i = 0, 1, 2$;
3. $n \equiv 1 \pmod 4$:
   a) $C_0(n) = C_1(n) \cap C_2(n)$;
   b) i. $C_0(n)$ is a $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ code and $C_0(n)^\perp$ is a $[\binom{n}{3}, \binom{n}{2}, n-2]_2$ code;
      ii. $C_1(n)$ is, for $n > 9$, a $[\binom{n}{3}, \binom{n}{3} - n + 1, 4]_2$ code and $C_1(n)^\perp$ is a $[\binom{n}{3}, n -$

$1, (n-2)(n-3)]_2$ *code, while* $C_1(9)$ *is a* $[84, 76, 3]_2$ *and* $C_1(9)^\perp$ *is a* $[84, 8, 38]_2$ *code ;*

iii. $C_2(n)$ *is a* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *code and* $C_2(n)^\perp$ *is a* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$ *code;*

c) $C_i(n) \cap C_i(n)^\perp = \{0\}$ *for* $i = 0, 1, 2$*;*

4. $n \equiv 3 \pmod 4$*:*

a) $C_1(n) = \langle v^P + j \mid P \in \mathcal{P} \rangle$ *of dimension* $\binom{n}{3} - 1$*;*

b) $C_0(n) = C_2(n)$ *is a* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *code, and* $C_2(n)^\perp$ *is a* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$ *code;*

c) $C_i(n) \cap C_i(n)^\perp = \{0\}$ *for* $i = 0, 1, 2$*.*

Furthermore, the automorphism groups of these codes are S_n *or* $S_{\binom{n}{3}}$

PD-sets for the codes

Result 9 (Key, Moori & Rodrigues [8]) *Let* $D = C_2(n)^{\perp}$ *be the*

$$[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$$

code from the design $\mathcal{D}_2(n)$ *when* $n \geq 7$ *is odd. Taking the points*

$$\{1, 2, n\}, \{1, 3, n\}, \ldots, \{n-2, n-1, n\}$$

as information symbols, but replacing the point $\{n-2, n-1, n\}$ *by* $\{n-3, n-2, n-1\}$, *then* D *has a PD-set in* S_n *given by the following elements of* S_n *in their natural action on triples of elements of* $\Omega = \{1, 2, \ldots, n\}$:

$$S = \{(n, i)(n-1, j)(n-2, k) \mid$$

$$1 \leq i \leq n, 1 \leq j \leq n-1, 1 \leq k \leq n-2\}.$$

Here D can correct $t = \frac{n-3}{2}$ errors.

The existence of a PD-set for a code is not invariant under equivalence: for example, in Result 9, the points

$$\{1, 2, n\}, \{1, 3, n\}, \ldots, \{n-2, n-1, n\}$$

can be taken as information symbols, but if they are, the code will not have a PD-set to correct all the allowed errors.

Example: For $n = 9$ the $[84, 14, 7]_2$ code corrects $t = 3$ errors but there is no element in S_9 that move the three points

$$\{1, 2, 9\}, \{3, 4, 5\}, \ldots, \{6, 7, 8\}$$

into the check positions. However, if $\{7, 8, 9\}$ is placed in the check positions and $\{6, 7, 8\}$ in the information positions, then it can be done: in this example, $(6, 9)$ will do it.

4. Projective planes

The desarguesian finite projective planes, $\Pi = PG_2(F_q)$, where $q = p^t$, give codes over F_p with dimension $\binom{p+1}{2}^t + 1$ and minimum weight $q+1$. The codes are subfield subcodes of the projective generalized Reed-Muller codes, and the automorphism groups are $P\Gamma L_3(q)$. In addition the codes are all cyclic, and the groups doubly transitive.

Thus PD-sets that correct two errors always exist. To find them, or to find PD-sets that will correct all the errors the code is capable of correcting, we need suitable information positions for these codes. Earlier work on finding bases for the codes (by Moorhouse [11] and Blokhuis and Moorhouse [1]) gives bases when $q = p$. Work in progress by Jirapha Limbupasiriporn has a tentative basis for $q = p^2$. With these bases, using for information positions the corresponding points in homogeneous coordinates, we can produce PD-sets to correct two errors in all cases.

Partial PD-set for projective planes of prime order

Let $\Pi = PG_2(F_p)$ where p is a prime, and let $C = C_p(\Pi)$. Then

$$C = [p^2 + p + 1, \binom{p+1}{2} + 1, p + 1]_p.$$

For $0 \leq s \leq p - 1$ let

$$\mathcal{C}_s = \{(0, 1, s)\} \cup \{(1, k, ks) \mid 1 \leq k \leq p - (s + 1)\},$$

and

$$\mathcal{I} = \bigcup_{s=0}^{p-1} \mathcal{C}_s \cup \{(1, 0, 0)\}.$$

Then $\mathcal{I}$ can be taken as the information symbols for C (by Moorhouse [11]) and the following set of matrices S will form a PD-set that will correct two errors.

Define, for $r, g, i \in F_p = F$,

$$B_{r,g,i} = \begin{bmatrix} 0 & 0 & 1 \\ 1-rg & -r & 1-ri \\ g & 1 & i \end{bmatrix}$$

and

$$C_{r,g,i} = \begin{bmatrix} 1 & 0 & 0 \\ -rg & -r & 1-ri \\ g & 1 & i \end{bmatrix}.$$

Let

$$S = \{C_{r,0,0}, C_{r,\pm 1,i}, C_{r,0,-1}, C_{r,1,-1} \mid r \in F, i \neq -1 \in F\} \cup$$

$$\{B_{r,0,0}, B_{r-1,0,-1}, B_{0,-1,1}, B_{0,-1,2} \mid r \in F\} \cup \{I_3\}.$$

S will act as a PD-set to correct two errors, and S contains $p^2 + 3p + 3$ elements.

References

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

[2] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994. http://www.maths.usyd.edu.au:8000/u/magma/.

[3] Hervé Chabanne. Permutation decoding of abelian codes. *IEEE Trans. Inform. Theory*, 38:1826–1829, 1992.

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

[5] 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.

[6] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples. Submitted.

[7] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes of triangular graphs and permutation decoding. Submitted.

[8] J. D. Key, J. Moori, and B. G. Rodrigues. Permutation decoding of binary codes from graphs on triples. In preparation.

[9] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. Submitted.

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

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

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

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